(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

BMVIT
Sektion III, Abteilung PT 2
Ghegastraße 1
1030 Wien
per E-mail: jd@bmvit.gv.at

Wien, am 15. Mai 2007

Betreff: Novelle des TKG
Umsetzung der Richtlinie über die Vorratsdatenspeicherung
GZ BMVIT-630.333/0001-III/PT2/2007

Sehr geehrte Damen und Herren!

In der Anlage übermitteln wir Ihnen unsere Stellungnahme zur Novelle des TKG im Rahmen der Umsetzung der Richtlinie über die Vorratsdatenspeicherung.

Für Rückfragen stehen wir gerne zur Verfügung.

Mit freundlichen Grüßen

europäisches zentrum für e-commerce und internetrecht
Data Retention Gruppe

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Stellungnahme im Rahmen des Begutachtungsverfahrens GZ BMVIT-630.333/0001-III/PT2/2007

Inhalt

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

I. Vorwort

Die Data Retention Richtlinie (DR-RL, 2006/24/EG) verpflichtet die Mitgliedstaaten eine verdachtsunabhängige Vorratsspeicherung von Standort- und Verkehrsdaten betreffend Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie umzusetzen.

Da diesem Akt des Sekundärrechts der EG ein Anwendungsvorrang gegenüber staatlichem Recht zukommt, kann die DR-RL nicht am Maßstab österreichischer Grundrechte geprüft werden. Der europäische Richtlinien-Geber ist jedoch gemäß Art 6 iVm Art 46 lit d EUV primärrechtlich an die Europäische Menschenrechtskonvention (EMRK) gebunden. Darüber hinaus ist die Republik Österreich unmittelbar aufgrund eines völkerrechtlichen Vertrages zur Einhaltung der EMRK verpflichtet. Im Folgenden soll daher eine Erörterung über die Frage der Zulässigkeit des durch die DR-RL bzw. ihre Umsetzung erfolgenden Eingriffs in die Grundrechte, insbesondere in Art 8 EMRK, vorgenommen werden.

Art 8 EMRK („Recht auf Achtung des Privat- und Familienlebens“) schützt in sehr allgemeiner Weise die Privatheit des Lebens gegen Kenntnisnahme durch den Staat, wozu der VfGH grundlegend ausführte: „In einer von der Achtung der Freiheit geprägten Gesellschaft wie sie die Präambel zur MRK voraussetzt, braucht der Bürger ohne triftigen Grund niemandem Einblick zu gewähren, welchem Zeitvertreib er nachgeht, welche Bücher er kauft, welche Zeitungen er abonniert, was er isst und trinkt und wo er die Nacht verbringt“[1].

Befürworter der Vorratsspeicherung sind bemüht zu betonen, dass es zu keiner Speicherung von Inhaltsdaten, sondern „lediglich“ zu einer Speicherung von Standort- und Verkehrsdaten kommt. Dem ist entgegenzuhalten, dass in vielen Fällen bereits durch Kenntnis des Kommunikationspartners ein Rückschluss auf den Inhalt der Kommunikation oder andere

[1] VfSlg 12.689/1991

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

sensible Elemente des Privatlebens möglich ist. Erhält jemand beispielsweise eine E-Mail von info@anonyme-alkoholiker.de, so kann (mit einer gewissen Wahrscheinlichkeit) angenommen werden, dass der Empfänger des E-Mails Alkoholprobleme hat. Telefoniert jemand regelmäßig – ausschließlich zu Ordinationszeiten – mit einem Kardiologen, so kann – wiederum mit einer bestimmten Wahrscheinlichkeit – angenommen werden, dass der Anrufer an einer Herz-Kreislauferkrankung leidet.

Das wahre Eingriffspotential einer flächendeckenden verdachtsunabhängigen Vorratsspeicherung von Standort- und Verkehrsdaten wird erst durch eine Illustration moderner Technologien, wie Data Mining deutlich. Data Mining bezeichnet ein komplexes Verfahren, in dessen Rahmen große Datenbestände nach wiederkehrenden Mustern durchsucht werden. Dies ermöglicht es beispielsweise durch die Frequenz der Kommunikation oder die Häufigkeit und Dauer des gemeinsamen Aufenthalts im Bereich einer Funkzelle (Cell-ID) soziale Beziehungen mit gewissen Wahrscheinlichkeiten zu rekonstruieren. Darüber hinaus ist es möglich ganze soziale Netze, ihre Ausbreitung sowie allfällige hierarchische Strukturen abzuleiten. Würden derartige Verfahren zur Kriminalitätsprävention eingesetzt, so käme es tatsächlich zu einer Ermittlung aller Personen, deren Kommunikationsprofil mit einer gewissen statistischen Wahrscheinlichkeit auf kriminelles Verhalten hinweist.

Derartige Ideen der Kriminalitätsprävention durch Überwachung sind meist von dem Gedanken getragen, dass mit einer umfangreichen Überwachung eine beinahe hundertprozentige Sicherheit erreichbar wäre. Dies ist jedoch nicht zutreffend. Keine noch so umfangreiche Überwachung wäre z.B. in der Lage einen Terroranschlag mit annähernd hundertprozentiger Sicherheit zu verhindern. Es drängt sich somit nicht nur aus rechtsdogmatischer, sondern insbesondere auch aus rechtspolitischer Sicht die Frage auf, in welchem Verhältnis die geminderte Wahrscheinlichkeit eines Terroranschlags (oder anderer schwerer Straftaten) zu den durch die Überwachung erfolgenden Eingriffen in die liberalen Grundrechte der Betroffenen stehen bzw. stehen sollten. Aus rechtspolitischer Sicht stellt sich die Frage, wie sich eine flächendeckende verdachtsunabhängige Überwachung der

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

Kommunikation der gesamten Bevölkerung auf die Entwicklung einer Gesellschaft auswirkt. Es ist zu erwarten, dass sich Personen alleine aufgrund der Tatsache, dass ihnen bewusst ist, dass ihre Verkehrs- und Standortdaten auf Vorrat gespeichert werden, anders verhalten werden. Diese Verhaltensmodifikation dieser Personen wird sich im überwachten Bereich daran orientieren, was als gesellschaftlich akzeptiertes Verhalten gilt und immer weniger daran, was ihren eigenen Ansichten oder moralischen Vorstellung entspricht. Die Einwirkung auf menschliches Verhalten ist notwendiger Bestandteil jeder Gesellschaft. Sie sollte jedoch primär durch die Schaffung von Rechtsnormen durch demokratisch legitimierte Rechtssetzungsorgane erfolgen. Durch weitreichende Überwachungsmaßnahmen werden Menschen aber indirekt zur Konformität und zur Änderung ihres Verhaltens bewegt, ohne dass dieser Prozess der Verhaltensmodifikation einem öffentlichen Diskurs und einer demokratischen Mitwirkung aller Betroffenen zugänglich wäre.

Dem Argument, dass rechtschaffene Bürger „ohnehin nichts zu verbergen hätten“ ist daher mit zweierlei Argumenten zu begegnen. Zum einen gilt, dass sehr viele Menschen im Bereich des rechtlich Zulässigen auch Handlungen setzen, von denen sie keineswegs wollen, dass sie Dritten bekannt werden (z.B. Anruf bei einer Selbsthilfe-Hotline). Insofern haben die meisten Menschen „etwas zu verbergen“. Zum anderen gilt, wie bereits ausgeführt wurde, dass eine weitreichende Überwachung nicht nur einen Eingriff in die Rechte konkreter Personen darstellt, sondern auch nachteilige gesellschaftliche Entwicklung bewirkt.

Aus den vorstehenden Erwägungen wird deutlich, dass bereits die (Vorrats-)Speicherung von Verkehrs- und Standortdaten einen schwerwiegenden Eingriff in die Privatsphäre darstellt. Dies gilt zunächst unabhängig davon, ob zu einem späteren Zeitpunkt eine Übermittlung oder Verarbeitung der Daten vorgesehen ist. Zum einen erfolgt die oben beschriebene Verhaltensanpassung allein aus dem Wissen um die Speicherung. Zum anderen wird die Ausweitung der Zugriffsmöglichkeiten durch Behörden auf bereits gespeicherte Daten in gesellschaftlichen Drucksituationen nicht zu verhindern sein.

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Erklärter Zweck der DR-RL ist die Ermittlung, Feststellung und Verfolgung von schweren Straftaten, einschließlich des Terrorismus. Dieses Ziel liegt grundsätzlich im öffentlichen Interesse und könnte daher geeignet sein, den Grundrechtseingriff zu rechtfertigen. Bezüglich des Ziels der Terrorismusbekämpfung ist jedoch zu betonen, dass sich in Österreich die Wahrscheinlichkeit eines Anschlages im Verhältnis zu den vergangenen Jahrzehnten wohl nur sehr geringfügig erhöht hat. Dies ist für die Frage, ob Österreich durch die Umsetzung der DR-RL eventuell Pflichten aus der EMRK verletzt, zu berücksichtigen, da hierbei die Bedrohungslage in anderen Mitgliedstaaten nicht relevant ist.

Da es – wie im Folgenden gezeigt werden wird – viele Bereiche gibt, in denen eine Vorratsspeicherung von Verkehrs- und Standortdaten in personenbezogener Form nicht erfolgt, erscheit es bereits fraglich, inwiefern die DR-RL überhaupt geeignet ist, das Ziel der Bekämpfung schwerer Straftaten zu erreichen. Die DR-RL beschränkt sich in ihrem Art 5 ausdrücklich darauf Verkehrs- und Standortdaten in Bezug auf die Bereiche Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie zu speichern. Daher ist die Kommunikation mittels HTTP (d.h. herkömmliches „Web-Surfen“), wie insbesondere die Kommunikation mit einem Web-Mail Service Provider (z.B. hotmail.com oder Gmail) oder einer Social Networking Website (z.B. MySpace.com) nicht erfasst. Ebenso wenig erfasst ist das File Transfer Protocol (FTP), das Protokoll Internet Relay Chat (IRC), alle Instant Messaging Protokolle (z.B. ICQ), File Sharing bzw. Peer2Peer-Protokolle, das Network News Transfer Protocol (NNTP) und Protokolle zur Remote-Administration wie SSH, Multimediaprotokolle wie RTSP oder RTP. Eine zweite Form der Umgehung besteht darin, anonyme Endgeräte wie öffentliche Telefonzellen, Wertkarten-Handys oder Internet-Cafes zu verwenden. Eine dritte Möglichkeit besteht in der Verwendung von Anonymisierungsdiensten, wie Tor. Es handelt sich hierbei um ein von der renommierten Bürgerrechtsorganisation EFF (Electronic Frontier Foundation) entwickeltes Programm, das auf weltweit über 450 sog Tor-Routern installiert ist und eine verschlüsselte Umleitung über jeweils drei Tor-Router ermöglicht, wodurch für den Empfänger der Nachricht nicht feststellbar ist, woher (bzw. von welcher IP-Adresse) die Nachricht ursprünglich kommt. Eine abschließend zu nennende – und aufgrund des engen Tatbestandes des § 118a StGB

((e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

nicht einmal strafbare – Umgehungsmöglichkeit besteht darin, ein fremdes Computersystem zu „hacken“ und von diesem aus zu kommunizieren.

Es gibt daher eine Fülle von Umgehungsmöglichkeiten, die jedem offen stehen und es ohne besondere Mühe ermöglichen die Vorratsspeicherung der Verkehrsdaten zu umgehen. Es ist daher mehr als wahrscheinlich, dass Personen, die für eine verdeckt operierende kriminelle bzw. terroristische Organisation tätig sind, Webmail anstatt POP3/SMTP oder überhaupt ICQ anstatt E-Mail, Wertkarten-Handys oder öffentlicher Telefonzellen anstatt regulärer Telefone und im Bereich des Internets Anonymisierungsdienste verwenden werden. Daher werden nur die Verkehrs- und Standortdaten jener Personen in personenbezogener Form erfasst werden können, die entweder über die Vorratsdatenspeicherung nicht informiert sind oder nicht über hinreichende Kenntnisse verfügen, um der Speicherung zu entgehen. Die Vorratsdatenspeicherung wird daher v.a. in die Grundrechte jener eingreifen, die eigentlich nicht Ziel der Überwachung sind. Denn kriminelle Organisation werden ihre Mitglieder vermutlich in die Lage versetzen, die Vorratsdatenspeicherung zu umgehen.

Vor diesem Hintergrund ist uE die Eignung der Vorratsdatenspeicherung zur Erreichung des Ziels der Bekämpfung der organisierten Kriminalität und des Terrorismus zu verneinen. Für den Bereich der Straftaten geringerer Schwere wäre eine Eignung uU zu bejahen. Ob eine flächendeckende verdachtsunabhängige Vorratsdatenspeicherung jedoch für diesen Bereich erforderlich ist, darf ernsthaft bezweifelt werden.

Darüber hinaus ist eine Prüfung der Verhältnismäßigkeit im engeren Sinn, dh eine Güterabwägung zwischen dem öffentlichen Interesse und dem Grundrechtseingriff vorzunehmen. Insbesondere in Bezug auf den Terrorismus gilt, dass für die Beurteilung des öffentlichen Interesses nicht nur die Schwere der Straftat, sondern auch die Wahrscheinlichkeit zu berücksichtigen ist, dass überhaupt eine solche Straftat begangen werden wird. Diese Wahrscheinlichkeit ist für das Staatsgebiet der Republik Österreich nicht signifikant gestiegen und daher äußerst gering. Alleine die Angst in der Bevölkerung vor einem – tatsächlich sehr unwahrscheinlichen – Anschlag durch Überwachungsmaßnahmen

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

zu mindern, ist jedoch kein öffentliches Interesse, das geeignet wäre einen Grundrechtseingriff dieses Umfangs zu rechtfertigen. Die Bekämpfung von Straftaten geringerer Schwere, deren Eintritt wesentlich wahrscheinlicher, wenn nicht sogar gewiss ist, stellt jedoch ein wesentlich geringeres öffentliches Interesse dar. Insbesondere kann uE die Bekämpfung von Vergehen iSd § 17 Abs 2 StGB keinesfalls eine flächendeckende verdachtsunabhängige Vorratsdatenspeicherung rechtfertigen. Aber auch die Bekämpfung von Verbrechen iSd § 17 Abs 1 StGB bietet uE in den seltensten Fällen eine hinreichende Rechtfertigung. Denn es ist zu berücksichtigen, dass durch umfangreiche Überwachungsmaßnahmen nicht nur ein massiver Eingriff in die Grundrechte eines jeden Einzelnen erfolgt, sondern darüber hinaus auch äußerst negative, in ihrem Umfang noch nicht abschätzbare Auswirkungen auf die Entwicklung unserer Gesellschaft entstehen können.

Die von der DR-RL vorgesehene Vorratsdatenspeicherung verletzt daher uE das in Art 8 EMRK normierte Grundrecht auf Achtung des Privatlebens. Da der EuGH aus Art 6 EUV ableitet, dass europäische Grundrechte, ähnlich jenen der EMRK Teil des Primärrechts sind, ist die DR-RL auf dieser Grundlage als gemeinschaftsrechtlich problematisch anzusehen. Es ist zu erwarten, dass nationale Höchstgerichte beim EuGH einen Antrag auf Vorabentscheidung stellen werden, wodurch der EuGH über diese Frage zu entscheiden haben wird. Weiters sind alle Mitgliedstaaten der Europäischen Union völkerrechtlich zur Einhaltung der EMRK verpflichtet. Es wäre daher auch denkbar, dass es auf Grundlage des Art 8 EMRK zu einer Verurteilung Österreichs oder anderer Mitgliedstaaten durch den Europäischen Gerichtshof für Menschenrechte (EGMR) kommt.

Weiters dürfte die DR-RL auch mit einer formellen Rechtswidrigkeit behaftet sein. Denn die Europäische Gemeinschaft verfügt nicht über die Kompetenz zur Erlassung von Richtlinien mit einem derartigen Inhalt. Es wurde versucht die Richtlinie auf die Binnenmarktkompetenz gemäß Art 95 EGV zu stützen, was angesichts des Regelungsinhalts der Richtlinie als rechtswidrig zu beurteilen ist. Denn der Schwerpunkt bzw. das Ziel der DR-RL ist nicht die Angleichung der nationalen Rechtsvorschriften, die das Funktionieren des Binnenmarkts

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

fördern, sondern eindeutig die Ermittlung, Feststellung und Verfolgung von schweren Straftaten. Dies wird insbesondere dadurch deutlich, dass die DR-RL die für einen funktionierenden Wettbewerb entscheidende Frage der Kostentragung nicht regelt. Da die Vorratsdatenspeicherung jedenfalls bezüglich der Standortdaten und dem Bereich des Internets nicht für die Erbringung einer Dienstleistung erforderlich ist, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken erfolgen soll, hat Irland vor dem EuGH eine Klage auf Nichtigerklärung (C-301/06) der DR-RL eingebracht. Da der EuGH den Ratsbeschluss 2004/496/EG über die Fluggastdatenübermittlung mit ähnlicher Argumentation für nichtig erklärt hat (C-317/04 und C-318/04), erscheint es nicht unwahrscheinlich, dass auch die DR-RL auf dieser Grundlage für nichtig erklärt werden wird.

II. Änderungsvorschläge

Die vorliegende Stellungnahme schlägt die folgenden Änderungen des Entwurfs vor:

- Korrektur eines **Redaktionsfehlers**: § 90 Abs 6 TKG 2003 ist entsprechend der Novellierung des § 92 Abs 3 Z 3 anzupassen, da die **Bonität** nicht unter die Auskunftspflicht fallen soll.
- Es sollte insbesondere aus grundrechtlichen Erwägungen **keine Ausweitung des Begriffs der Stammdaten** erfolgen. In § 92 Abs 3 Z 3 lit a sollte der Verweis auf „Daten gemäß Z 4a lit. a“ daher gestrichen werden. Es wird empfohlen, § 92 Abs 3 Z 3 lit d TKG 2003 („Teilnehmernummer und sonstige Kontaktinformation für die Nachricht“) beizubehalten.
- Korrektur eines **Redaktionsfehlers**: § 92 Abs 4a sollte als § 92 Abs 3 Z 4b bezeichnet werden.
- Um Rechtsunsicherheiten zu vermeiden, sollte einstweilen von der Einführung einer **Speicherpflicht in Bezug auf Internetzugang, Internet-E-Mail und Internet-Telefonie** abgesehen werden. § 92 Abs 4a lit a sublit bb wäre entsprechend zu streichen.

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

- Die Datenspeicherung in Bezug auf die **Erstaktivierung** eines vorbezahlten anonymen Dienstes hat gemäß Art 5 Abs 1 lit e Z 2 DR-RL **nur für** den Bereich des **Mobilfunks** zu erfolgen. § 92 Abs 4a lit e sublit cc ist daher unter § 92 Abs 4a lit e sublit bb als sechster Spiegelstrich einzugliedern.
- **Die Übermittlung als auch die Verarbeitung von auf Vorrat gespeicherter Daten sollte nur unter einem Richtervorbehalt zulässig sein**. Eine Verarbeitung auf Grundlage des § 53 Abs 3a Satz 1 SicherheitspolizeiG, des § 22 Abs 2a MilitärbefugnisG oder § 87b Abs 3 Urheberrechtsgesetz ist entschieden abzulehnen. Die Verwendung (§ 4 Z 20 DSG 2000) der auf Vorrat gespeicherten Daten hat daher ausschließlich zu dem Zweck der Erfüllung der nach der StPO iVm § 94 Abs 2 TKG 2003 bestehenden Mitwirkungspflichten zu erfolgen.
- Korrektur eines **Redaktionsfehlers**: § 102a Abs 1 verweist bezüglich der auf Vorrat zu speichernden Daten auf „§ 92 Abs 3 Z 4a“, wohingegen die Definition des Begriffs der Vorratsdaten in § 92 Abs 4a erfolgt.
- Die in § 102b normierten **Auskunftspflichten** haben **unabhängig davon** zu bestehen, **ob** die Daten **rechtmäßiger** Weise weitergegeben wurden – d.h. an die zuständige Behörde und im Einklang mit den Bestimmungen der StPO.
- Korrektur eines **Redaktionsfehlers**: In § 102a Abs 4 und § 137 Abs 2 sollte auf § 114a und nicht auf § 114 TKG 2003 verweisen werden.
- **Bezüglich** der Erfüllung der **Auskunftspflichten** nach § 102b ist nach dem Verhältnismäßigkeitsgrundsatz eine **Regelung über die Kostentragung erforderlich**.
- Die Übermittlung der auf Vorrat gespeicherten Daten gemäß § 149a Abs 2 StPO bzw. § 135 Abs 2 StPO idF BGBl I Nr 19/2004 sollte **ohne Zustimmung des Anschlussinhabers** erst zur Aufklärung eines **Verbrechens iSd § 17 Abs 1 StGB**, d.h. einer vorsätzlichen Handlung, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht ist, zulässig sein. **Mit Zustimmung des Anschlussinhabers** sollte eine Datenübermittlung nur zur Aufklärung einer **vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung** zulässig sein.

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

- Bezüglich der gesamten Vorratsdatenspeicherung ist eine **Regelung über die Kostentragung verfassungsrechtlich geboten**. § 102a sollte daher in einem neuen Abs 5 um eine § 94 Abs 2 TKG 2003 entsprechende Bestimmung erweitert werden. **Es ist unzutreffend, dass keine zusätzlichen Speicherpflichten bzw. Mehrkosten entstehen würden.**

Alle Paragraphenbezeichnungen beziehen sich, sofern nicht anders angegeben auf den vorliegenden Entwurf zur Novellierung des TKG 2003.

1. Zu § 92 Abs 3 Z 3

Äußerst problematisch erweist sich der in § 92 Abs 3 Z 3 lit a aufgenommene Verweis auf „Z 4a lit. a“. Da § 92 Abs 3 Z 4a TKG 2003 nicht novelliert werden soll und nur den Begriff der Zugangsdaten definiert, sowie darüber hinaus gar keine lit a enthält, ist anzunehmen, dass ein Verweis auf § 92 Abs 4a lit a beabsichtigt war. In den Erläuterungen wird hierzu ausgeführt, dass normiert werden soll, „dass dynamische IP-Adressen zu den Stammdaten zählen“. Dies hätte der Oberste Gerichtshof nach Ansicht der Verfasser des Entwurfs ohnedies bereits in einem Urteil vom 26.7.2005 (11 Os 57/05z, 11 Os 58/05x und 11 Os 59/05v) klargestellt. Im Folgenden soll gezeigt werden, dass der OGH im erwähnten Urteil eine derartige Aussage *nicht* trifft. Darüber hinaus hätte eine Erweiterung des Begriffs der Stammdaten um die nach § 92 Abs 4a lit a zu speichernden Daten – bei denen es sich nach allgemeinen Grundsätzen um Verkehrsdaten handelt – schwerwiegende Auswirkungen.

In dem Urteil 11 Os 57/05z hatte der OGH zu entscheiden, unter welchen Vorraussetzungen ein Telekommunikationsdiensteanbieter Name und Anschrift eines Anschlussinhabers anhand einer IP-Adresse zu ermitteln und dem Gericht auf gerichtliche Anordnung zu übermitteln hat. Entscheidend ist hierbei, dass nicht die IP-Adresse (ein Verkehrsdatum), sondern Name und Anschrift (Stammdaten) zu übermitteln waren. Der OGH führte aus:

„Im vorliegenden Fall ist die Privatanklägerin […] bereits in Kenntnis der

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

Internetadresse, von der aus der Verdächtige agiert hat. Ihr Auskunftsbegehren zielt lediglich dahin, Namen und Anschrift desjenigen Kunden des Access Providers in Erfahrung zu bringen, dem diese Adresse in einem bestimmten Zeitraum zugeordnet war, maW auf Stammdaten iSv § 92 Abs 3 lit a, lit c TKG 2003. […] § 149a Abs 1 Z 1 lit b StPO stellt auf die sogenannte „Rufdatenrückerfassung" ab, durch die offen gelegt wird, wann, wie lange und mit welchen Teilnehmern an der öffentlichen Telekommunikation mittels einer bestimmten Anlage aktiv oder passiv Verbindung aufgenommen wurde […]. Eine derartige Offenlegung ist bei der Mitteilung der in Rede stehenden Stammdaten des Benutzers einer IP-Adresse zu einer bestimmten Zeit nicht erforderlich."

Da der OGH auch das Vorliegen einer planwidrigen Lücke verneinte, erklärte er § 149a StPO für den vorliegenden Fall als nicht anwendbar, weswegen die Übermittlung des Namens und der Anschrift des Inhabers eines bereits individualisierten Anschlusses auf Grundlage des § 102 Abs 4 TKG 2003 formlos zu erfolgen habe. Der OGH hat damit eine Anwendbarkeit des § 149a StPO nicht deshalb verneint, weil dynamische IP-Adressen als Stammdaten zu beurteilen wären, sondern weil ausschließlich eine Übermittlung des Namens und der Anschrift (somit von Stammdaten) vom Gericht aufgetragen wurde. Die Subsumtion dynamischer IP-Adressen unter den Begriff „Stammdaten" überschreitet uE nach geltender Rechtslage den äußerst möglichen Wortsinn des § 92 Abs 3 Z 4a TKG 2003.

§ 92 Abs 3 Z 4a TKG 2003 definiert Zugangsdaten als *„jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind"*. Eine neu zuzuweisende dynamische IP-Adresse wird im Rahmen der Herstellung des Internetzugangs in einem vom Provider betriebenen DHCP-Server[2] errechnet – sie „entsteht" daher „beim Betreiber". Die zugewiesene IP-Adresse wird in weiterer Folge vom Computersystem des Anschlussinhabers as Quell-Adresse in jedem versendeten IP-Paket

[2] Dynamic Host Configuration Protocol, spezifiziert in RFC 2131

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

angegeben. Eine IP-Adresse kann nicht nur für die Zuordnung von versendeten IP-Paketen zu dem Anschluss des Versenders, sondern auch für die Zuordnung von IP-Paketen zu dem Anschluss des Empfängers verwendet werden. Andere Systeme verwenden daher spiegelbildlich besagte IP-Adresse als Ziel-Adresse für IP-Pakete, die an das Computersystem des Anschlussinhabers zu übermitteln sind.[3] Eine dynamische IP-Adresse ist somit auch für „die Zuordnung der […] verwendeten Netzwerkadressierungen zum Teilnehmer" notwendig. Da IP-Adressen im Rahmen des IP-Routings für Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz verarbeitet werden[4], sind dynamische IP-Adressen Verkehrsdaten iSd § 92 Abs 3 Z 4 TKG 2003 und im Besonderen Zugangsdaten iSd § 92 Abs 3 Z 4a TKG 2003.

Zu diesem Ergebnis gelangt auch die Empfehlung K213.000/0005-DSK/2006 der Datenschutzkommission (DSK). In Übereinstimmung mit dieser ist die Entscheidung des OGH in dem Punkt zu kritisieren, dass gänzlich vernachlässigt wurde, dass die an sich zulässige Übermittlung der Stammdaten nach § 90 Abs 6 TKG 2003 im entscheidungsgegenständlichen Fall in einem vorgelagerten ersten Schritt die Verarbeitung iSd § 4 Z 9 DSG 2000 der dynamischen IP-Adresse, dh eines Verkehrsdatums erfordert. Die DSK führt hierzu in ihrer Empfehlung aus, dass dynamische IP-Adressen gemäß § 99 Abs 1 TKG 2003 nach Beendigung der Einwahl-Verbindung grundsätzlich zu löschen sind. Darüber hinaus ist anzumerken, dass auch die Verarbeitung der Verkehrsdaten – als vorgelagerter Schritt zur Übermittlung der Stammdaten – gemäß § 92 Abs 1 TKG 2003 iVm § 7 Abs 1 DSG 2000 einer Zweckbindung unterliegt. Da § 103 Abs 4 TKG 2003 die Zweckbindung nur in Bezug auf jene Daten ausweitet, die in ein Teilnehmerverzeichnis aufzunehmen sind, hätte die dynamische IP-Adresse als Verkehrsdatum nicht verarbeitet werden dürfen, wodurch im Ergebnis das Bestehen einer Auskunftspflicht gegenüber dem Gericht uE zu verneinen gewesen wäre.

---

[3] *Stevens*, TCP/IP Illustrated, Volume 1, 33 ff

[4] *Stevens*, TCP/IP Illustrated, Volume 1, 37 ff

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Der Entwurf sieht jedoch vor, dass „Daten gemäß Z 4a lit a“ (gemeint ist, wie bereits ausgeführt Abs 4a lit a) nun als Stammdaten zu gelten hätten. Der im Entwurf enthaltene Verweis auf § 92 Abs 4a lit a erfasst alle „zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigten Daten“, somit u.a. auch E-Mail-Adressen (gemäß § 92 Abs 4a lit a sublit bb 1. Spiegelstrich betreffend Internet-E-Mail) und VoIP-Adressen (gemäß § 92 Abs 4a lit a sublit bb 1. Spiegelstrich betreffend Internet-Telefonie) und zwar auch dann, wenn diese Adressen in keinerlei Zusammenhang mit einem vom Provider angebotenen E-Mail- oder VoIP-Dienst stehen. Bei den nach § 92 Abs 4a lit a zu speichernden Daten handelt es sich aus Sicht des speicherpflichtigen Providers nach allgemeinen Grundsätzen zweifelsfrei um Verkehrsdaten – und keine Stammdaten.

Der Entwurf sieht somit vor bestimmte Verkehrsdaten zu Stammdaten zu erklären. Hierdurch wird jedoch ein Widerspruch zwischen dem ersten und dem zweiten Halbsatz des § 92 Abs 3 Z 3 erzeugt. § 92 Abs 3 Z 3 1. Halbsatz definiert Stammdaten als *„alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind“*. Die von einem Kunden im Zusammenhang mit dem Dienst eines vom speicherpflichtigen Anbieter verschiedenen Anbieters[5] verwendete E-Mail- oder VoIP-Adresse ist jedoch ebenso wenig, wie eine dynamische IP-Adresse für die Begründung, Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen erforderlich. Selbiges gilt für die Erstellung und Herausgabe eines Teilnehmerverzeichnisses. § 92 Abs 3 Z 3 2. Halbsatz nennt durch den Verweis auf § 92 Abs 4a lit a Daten, die die Anforderungen des 1. Halbsatzes nicht erfüllen, insofern ein Widerspruch vorliegt. Da dieser Widerspruch, dass bestimmte Verkehrsdaten nach dem 1. Halbsatz keine, jedoch nach dem 2. Halbsatz sehr wohl Stammdaten sein

[5] Eine E-Mail-Adresse wird z.B. ausschließlich im Zusammenhang mit dem Dienst eines anderen Anbieters verwendet, wenn der POP3- bzw. IMAP-Server nicht vom Access Provider, sondern von einem anderen Anbieter betrieben wird und darüber hinaus nicht der SMTP-Server des Access Providers, sondern jener des anderen Anbieters zum Einsatz kommt.

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

sollen, nicht aufgelöst werden kann, sind an der der erforderlichen Bestimmtheit dieser Regelung iSd Art 18 Abs 1 B-VG erhebliche Zweifel angebracht.

Daten, die nach geltender Rechtslage unter den Begriff der Verkehrsdaten zu subsumieren sind, in Zukunft als Stammdaten zu bezeichnen, wirft darüber hinaus erhebliche – teils verfassungsrechtliche – Probleme auf. So gilt insbesondere, dass alle Stammdaten iSd § 92 Abs 3 Z 3 lit a bis e TKG 2003 gemäß § 90 Abs 6 TKG 2003 von einer Auskunftspflicht gegenüber Verwaltungsbehörden erfasst sind. Es ist ausreichend, dass eine solche Behörde im Rahmen eines schriftlichen und begründeten Verlangens darlegt, dass der betreffende Teilnehmer unter dem Verdacht steht „durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben“. Weiters wären jene Daten, die nach geltender Rechtslage als Verkehrsdaten anzusehen sind und nach dem Entwurf künftig als Stammdaten zu gelten hätten nicht mehr vom Kommunikationsgeheimnis gemäß § 92 Abs 1 TKG 2003 geschützt.

Sollten daher wie bisher im Entwurf vorgesehen, alle Daten iSd § 92 Abs 4a lit a als Stammdaten definiert werden, würde die Vorratsdatenspeicherung im Ergebnis nicht wie in Art 1 Abs 1 DR-RL vorgesehen für den Zweck der Ermittlung, Feststellung und Verfolgung von „*schweren Straftaten*“, sondern bereits von Verwaltungsübertretungen erfolgen. Ein derartig gravierender Grundrechtseingriff zu Zwecken der Bekämpfung von Verwaltungsübertretungen erscheint verfassungsrechtlich äußerst bedenklich.

Die oben dargestellten Bedenken werden weiters dadurch verstärkt, dass wie noch unter II.2. auszuführen sein wird, die Verwendung von dynamischen IP-Adressen ohne zugehörigen Zeitpunkt zu dem sie zugewiesen wurden keinen Sinn ergibt, insofern eine Eignung zur Erreichung des öffentlichen Interesses zu verneinen ist. Eine Eignung würde allenfalls dann bestehen, wenn auch die zugehörigen Zeitangaben (Daten gemäß § 92 Abs 4a lit c) zu übermitteln wären. Ein derart geeigneter Eingriff in das Grundrecht auf Privatsphäre wäre jedoch so schwer, dass uE eine Verhältnismäßigkeit ieS zur Bekämpfung von Verwaltungsübertretungen zu verneinen wäre.

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Zur Vermeidung von Rechtsunsicherheiten sollte zur Gänze von dem gemäß Art 15 Abs 3 DR-RL erklärten Vorbehalt Gebrauch gemacht und die Umsetzung der DR-RL in Bezug auf den Bereich des Internets bis März 2009 aufgeschoben werden. Dies gilt insbesondere, aufgrund der grundrechtlichen Sensibilität der Materie. Weiters sei auf die unter Ausführungen unter II.2.3. verwiesen.

Es wird empfohlen, § 92 Abs 3 Z 3 lit d TKG 2003 beizubehalten, in § 92 Abs 3 lit a ausschließlich *„Name und Anschrift“* zu nennen, die Bonität unter lit d zu normieren und für die Legaldefinition der Begriffe „Name“ und „Anschrift“ die Ziffern 11 und 12 einzuführen:

11. „Name“ Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen;
12. „Anschrift“ Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen.

Bezüglich § 92 Abs 3 Z 3 lit d ist den Erläuterungen zu entnehmen, dass lediglich eine Neubezeichnung der bisherigen lit e und f erfolgen soll. Hierbei ist offenbar § 90 Abs 6 TKG 2003 übersehen worden, der eine Auskunftspflicht bezüglich der in § 92 Abs 3 Z 3 lit a bis e aufgezählten Daten normiert. Um die Bonität – wie nach geltender Rechtslage – aus der Auskunftspflicht auszuschließen, sollte in § 90 Abs 6 der Verweis auf *„§ 92 Abs. 3 Z 3 lit. a bis e“* durch *„§ 92 Abs. 3 Z 3 lit. a bis c“* ersetzt werden. Sollte § 92 Abs 3 Z 3 lit d TKG 2003 übernommen werden und die Bonität dadurch unter lit e genannt werden, so wäre der Verweis auf *„§ 92 Abs. 3 Z 3 lit. a bis e“* durch *„§ 92 Abs. 3 Z 3 lit. a bis d“* zu ersetzen.

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

2. Zu § 92 Abs 4a

Nach dem Entwurf soll eine Legaldefinition des Begriffs der Vorratsdaten in § 92 Abs 4a erfolgen. Da § 92 Abs 3 in Z 1 bis 10 Legaldefinitionen enthält und er darüber hinaus keinen Abs 4 kennt, ist davon auszugehen, dass es sich um einen Redaktionsfehler handelt und die neue Legaldefinition tatsächlich in § 92 Abs 3 Z 4b erfolgen sollte. Im Folgenden wird dennoch bezüglich des Begriffs der Vorratsdaten weiter auf § 92 Abs 4a verwiesen.

§ 92 Abs 4a definiert die gemäß § 102a auf Vorrat zu speichernden Daten. Besonders problematisch erscheint die Speicherung von zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigten Daten betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie (§ 92 Abs 4a lit a sublit bb). Aus den Erläuterungen ist zu entnehmen, dass diese - aufgrund des gemäß Art 15 Abs 3 DR-RL erklärten Vorbehalts noch nicht erforderliche – Speicherpflicht zur rechtlichen Klarstellung und „Vermeidung von Missverständnissen“ erfolgen soll. Das Gegenteil ist jedoch der Fall.

2.1. Auslegungsprobleme in Bezug auf die Löschungspflicht nach sechsmonatiger Speicherung

Wie sich aus den Erläuterungen ergibt, dürfen Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung (Art 5 Abs 1 lit c DR-RL) betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie nicht gespeichert werden. Selbiges ergibt sich e contrario aus § 92 Abs 4a lit c. Wie soll jedoch eine Löschung der Daten gemäß § 102a Abs 1 nach sechs Monaten erfolgen, wenn nicht gespeichert werden darf, wann eine Nachrichtenübermittlung erfolgt ist?

Aus dem Gebot den Grundrechtseingriff möglichst gering zu halten ergibt sich das Erfordernis die Speicherdauer zu beschränken und hieraus die Notwendigkeit, Datum und Uhrzeit gemäß § 102a Abs 1 festzuhalten. Diese Speicherpflicht ist daher so auszulegen, dass der Grundrechtseingriff möglichst gering ausfällt.

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

((e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Bei der Beurteilung der Schwere des erfolgenden Grundrechtseingriffs sind Inhalt und Umfang der gespeicherten Daten sowie die Speicherdauer gegeneinander abzuwägen. Um die Speicherdauer von sechs Monaten nicht zu überschreiten, müsste das Datum und die Uhrzeit der Nachrichtenübermittlung gespeichert werden.

Für den Bereich der dynamischen IP-Adressen[6] ermöglicht erst die exakte Speicherung des Zeitpunkts jeder Nachrichtenübermittlung die Feststellung welchem Anschluss eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Erfolgt daher keine Speicherung des exakten Zeitpunkts, ist die Vorratsdatenspeicherung von dynamischen IP-Adressen für die Zuordnung einer zu einem bestimmten Zeitpunkt erfolgten Verbindung zu einem konkreten Anschlussinhaber nicht zu gebrauchen.

Dessen ungachtet handelt es sich hierbei um personenbezogene Daten, da festgestellt werden kann, welche IP-Adressen einem Anschlussinhaber in den letzten sechs Monaten zugewiesen waren. Aufgrund dieser Qualifikation als personenbezogene Daten, haben die Betroffenen ein rechtlich geschütztes Interesse, dass die sechsmonatige Speicherdauer eingehalten wird bzw. wenn unumgänglich nur in möglichst geringem Ausmaß überschritten wird. Zum anderen besteht das scheinbar gegenläufige Interesse die für die zeitgerechte Löschung erforderliche Uhrzeit, inklusive Datum, nicht zu speichern.

Der aufgrund der Speicherung des Datums der Nachrichtenübermittlung erfolgende Grundrechtseingriff lässt sich dadurch minimieren, dass nicht ein bestimmter Tag oder eine Uhrzeit, sondern ein mehrtätiger Zeitraum als Zeitangabe gewählt wird. Würde beispielsweise jede Nachrichtenübermittlung auf 23:59:59 des letzten Tages der Woche datiert, so würde dies dazu führen, dass manche Daten bis zu sieben Tage länger als sechs Monate gespeichert würden. Da im Gegenzug aus der Angabe eines bestimmten Zeitpunktes und einer bestimmten dynamischen IP-Adresse kein konkreter Anschluss mehr ermittelbar

[6] Eine dynamische Internet Protokoll (IP) Adresse wird einem Anschluss nur für die Dauer einer aufrechten Internetverbindung zugewiesen. Bei Wiederherstellung der Internetverbindung wird einem Anschluss idR eine neue IP-Adresse (aus demselben Adress-Pool) zugewiesen.

((e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

ist, stellt dies einen geringeren Grundrechtseingriff als die präzise Speicherung des Datums und der Uhrzeit der Nachrichtenübermittlung dar.

Im Widerspruch zu dieser Auslegung könnte eine verfassungskonforme Interpretation vorgebracht werden. Denn wenn nur ein mehrtägiger Zeitraum gespeichert wird, so stellt sich die Frage nach der Eignung dieses Mittels zur Erreichung des Zwecks der Verbrechensbekämpfung. Nach der oben dargestellten Auslegung, die nur die Speicherung eines mehrtägigen Zeitraums ermöglicht, wäre der hier beschriebene Grundrechtseingriff mangels sachlicher Rechtfertigung verfassungswidrig. Der Grundrechtseingriff wäre allenfalls nur dann verfassungskonform, wenn die präzise Speicherung des Datums und der Uhrzeit einer Nachrichtenübermittlung erfolgen würde, da erst mit dieser Handhabung eine konkrete Ermittlung, Feststellung und Verfolgung möglich wäre. Aus den Erläuterungen ist durch den Verweis auf die Empfehlung der Datenschutzkommission vom 11. Oktober 2006, GZ K213.000/0005-DSK/2006 ersichtlich, dass die Ermittlung eines konkreten Anschlusses aufgrund einer in der Vergangenheit verwendeten dynamischen IP-Adresse wohl ermöglicht werden sollte. Das Ergebnis dieser verfassungskonformen Interpretation würde jedoch über den äußerst möglichen Wortsinn des § 92 Abs 4a hinaus gehen.

Zusammenfassend ist anzumerken, dass durch § 92 Abs 4a lit a sublit bb bzw**.** durch die fehlende Erwähnung von Internetzugang, Internet-E-Mail und Internet-Telefonie in § 92 Abs 4a lit c eine beträchtliche Rechtsunsicherheit in einem grundrechtlich höchst sensiblen Bereich geschaffen würde.

2.2. Beurteilung der Verfassungskonformität

Da § 92 Abs 4a aus den oben erörterten Gründen wohl so auszulegen ist, dass nicht der Zeitpunkt, sondern nur ein gewisser Zeitraum zu speichern ist, in dem die Nachrichtenübermittlung erfolgte, stellt sich die Frage, ob diese Form der Vorratsspeicherung geeignet ist, den Eingriff in das Grundrecht auf Achtung des Privatlebens

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

gemäß Art 8 EMRK zu rechtfertigen. Da wie bereits erwähnt die Speicherung der Zuweisung einer dynamischen IP-Adresse ohne präzise Zeitangabe keine für die Kriminalitätsbekämpfung dienliche Auswertung ermöglicht, ist eine Eignung dieses Mittels jedenfalls in Bezug auf den Bereich des Internetzugangs zu verneinen. In Bezug auf Internetzugang, Internet-E-Mail und Internet-Telefonie ist es nicht möglich sich auf den Anwendungsvorrang der DR-RL zu berufen, da Österreich einen Vorbehalt gemgemäß Art 15 Abs 3 DR-RL erklärt hat, wodurch bis zum 15. März 2009 ein Umsetzungsspielraum besteht, dessen Ausübung am Maßstab des österreichischen Verfassungsrechts, wie insbesondere der Grundrechte nach EMRK zu prüfen ist. Mangels Verhältnismäßigkeit des Eingriffs in Art 8 EMRK wäre § 92 Abs 4a in der derzeit vorgeschlagenen Form daher wohl verfassungswidrig.

2.3. Änderungsvorschläge

Um die oben beschriebene Rechtsunsicherheit und die uE gegebene Verfassungswidrigkeit zu beseitigen, bestehen zwei Möglichkeiten:

Die erste Möglichkeit besteht darin, auch bezüglich des Internetzugangs zu normieren, dass Datum, Uhrzeit und Dauer der Nachrichtenübermittlung zu speichern sind. Aufgrund der Tatsache, dass die Unsicherheiten der technischen Entwicklung im Bereich Internet-E-Mail und Internet-Telefonie noch zu groß sind, wird jedenfalls empfohlen von einer Vorratsspeicherung betreffend Internet-E-Mail und Internet-Telefonie abzusehen. Denn insbesondere im Bereich E-Mail und VoIP wäre die Erfüllung der Speicherpflichten mit einem verhältnismäßig hohen finanziellen Aufwand verbunden. Sollte man sich entscheiden, die Identifizierung der Quelle einer Nachricht zu ermöglichen, so schlagen wir vor, dies auf den Bereich des Internetzugangs zu beschränken und *„Internet-E-Mail und Internet-Telefonie“* aus § 92 Abs 4a lit a sublit bb zu streichen. Um eine Speicherpflicht von Datum und Uhrzeit bezüglich des Internetzugangs zu normieren, sollte § 92 Abs 4a lit c um einen Spiegelstrich erweitert werden: *„- betreffend Internetzugang: Datum und Uhrzeit der An- und Abmeldung*

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers;“.

Die zweite Möglichkeit, der uE der Vorzug zu geben ist, besteht darin, zur Gänze von dem gemäß Art 15 Abs 3 DR-RL erklärten Vorbehalt Gebrauch zu machen. Insbesondere aus folgenden Gründen wird daher empfohlen die Umsetzung der Richtlinie in Bezug auf Internetzugang, Internet-E-Mail und Internet-Telefonie gemäß Art 15 Abs 3 DR-RL erst bis 15. März 2009 durchzuführen:

- Im Bereich des Internets ist die Vorratsdatenspeicherung im Verhältnis zum Bereich der Telefonie mit einem sehr großen finanziellen Aufwand verbunden.
- Würde die Umsetzung der Richtlinie in Bezug auf Internetzugang, Internet-E-Mail und Internet-Telefonie, wie derzeit geplant in zwei Etappen erfolgen, so fielen unnötiger Weise zweimal Planungs- und Umstellungskosten seitens der Anbieter und Betreiber an.
- Wie auch in den Erläuterungen erwähnt, wäre es vorteilhaft weitere technische Entwicklungen abzuwarten. Damit wäre es möglich von den Erfahrungen anderer Mitgliedstaaten bei der gänzlichen Umsetzung der Richtlinie zu profitieren.
- Eine übereilte Umsetzung der DR-RL würde zu erheblichen Wettbewerbsnachteilen österreichischer Internet Service Provider gegenüber ausländischen Konkurrenten führen.

Es wird daher empfohlen § 92 Abs 4a lit a sublit bb gänzlich zu streichen.

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

3. Zu § 92 Abs 4a lit e

In Bezug auf jene Daten, die bei der Erstaktivierung eines vorbezahlten anonymen Dienstes zu speichern sind, ist zu betonen, dass Art 5 Abs 1 lit e Z 2 DR-RL eine Speicherung nur betreffend Mobilfunk vorsieht. § 92 Abs 4a lit e sublit cc sollte daher unter § 92 Abs 4a lit e sublit bb als sechster Spiegelstrich eingegliedert werden. Eine Speicherpflicht im Rahmen der Erstaktivierung vorbezahlter anonymer Dienste würde ohne Einschränkung auf den Mobilfunk-Bereich zu einer nicht abschätzbaren Ausweitung der Speicherpflichten führen. Hierbei wäre beispielsweise an vorbezahlte mobile Mail-Clients, ähnlich einem BlackBerry zu denken, die nach Art 5 Abs 1 lit e Z 2 DR-RL jedenfalls nicht erfasst wären.

4. Zu § 102a Abs 1

§ 102a Abs 1 enthält einen redaktionellen Fehler, da bezüglich der auf Vorrat zu speichernden Daten auf „§ 92 Abs. 3 Z 4a“ verwiesen wird. Der Begriff der Vorratsdaten wurde jedoch in § 92 Abs 4a definiert, der wie unter II.2. ausgeführt wird, darüber hinaus richtigerweise als § 92 Abs 3 Z 4b zu bezeichnen wäre. Der Verweis auf *„§ 92 Abs. 3 Z 4a“* ist daher durch *„§ 92 Abs. 3 Z 4b“* zu ersetzen, andernfalls nur Zugangsdaten iSd § 93 Abs 3 Z 4a TKG 2003 auf Vorrat zu speichern wären.

Nach § 102a Abs 1 soll die Speicherung „zum Zwecke der Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17 SPG), einschließlich der Tatbestände der §§ 107 und 107a StGB“ erfolgen.

Dieser Zweck ist in mehrerlei Hinsicht problematisch. § 17 SPG definiert mit beträchtlicher Strafe bedrohte Handlungen als „gerichtlich strafbare Handlungen, die mit mehr als einjähriger Freiheitsstrafe bedroht sind“, ohne eine vorsätzliche Begehung zu erfordern. Die Übermittlung der gemäß § 102a Abs 1 gespeicherten Daten an die Kriminalpolizei hat

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

gemäß § 149a Abs 2 Z 1 oder 2 StPO iVM § 149b StPO (bzw. gemäß § 135 Abs 2 StPO idF BGBl I Nr 19/2004) zu erfolgen. Der in § 102a Abs 1 enthaltene Speicherzweck ist in Bezug auf die genannten Bestimmungen der StPO jedoch einerseits zu weit, andererseits zu eng.

Der auf § 17 SPG bezogener Zweck ist zu weit gefasst, da § 149a Abs 2 Z 1 und 2 StPO (so auch § 135 Abs 2 Z 1 bis 3 StPO idF BGBl I Nr 19/2004) eine vorsätzlich begangene Straftat erfordern, wohingegen nach § 17 SPG bereits eine fahrlässig Begehung ausreichend ist. Ungeachtet der weiten Formulierung des Art 1 Abs 1 DR-RL sind jedoch fahrlässig begangene Straftaten uE jedenfalls keine „schweren Straftaten“ iSd DR-RL.

In Bezug auf die Frage welche Straftaten „schwere Straftaten“ iSd DR-RL darstellen, bleibt dem österreichischen Gesetzgeber ein gewisser Spielraum. Innerhalb dieses Spielraums könnte die doppelte Normbindung des Gesetzgebers schlagend werden und eine Überprüfung der Umsetzung im Lichte des Art 8 EMRK erfolgen. Da das öffentliche Interesse an der Ermittlung, Feststellung und Verfolgung von Fahrlässigkeitsdelikten im Vergleich zur Schwere des Grundrechtseingriffs äußerst gering ist, wird eine Verhältnismäßigkeit (im engeren Sinn) des Eingriffs zu verneinen sein. Ein auf § 17 SPG bezogener Speicherzweck ist daher als verfassungswidrig zu beurteilen.

Der in § 102a Abs 1 genannte Zweck ist andererseits auch zu eng gefasst, da er eine Handlung erfordert, die mit mehr als einjähriger Freiheitsstrafe bedroht ist. Dies steht im Widerspruch zu § 149a Abs 2 Z 1 StPO (so auch § 135 Abs 2 Z 2 StPO idF BGBl I Nr 19/2004), wonach bei Zustimmung des Inhabers des Teilnehmeranschlusses bereits eine mit mehr als sechsmonatiger Freiheitsstrafe bedrohte Vorsatztat ausreicht.

Die genannten Probleme verdeutlichen, dass §§ 102a f in einem untrennbaren Zusammenhang mit jenen Bestimmungen stehen, die eine Verarbeitung oder Übermittlung der nach § 102a Abs 1 gespeicherten Daten ermöglichen. Hierbei ist festzustellen, dass in den Erläuterungen ausdrücklich darauf hingeweisen wird, dass eine Überlassung der Daten nur nach den Bestimmungen der StPO erfolgen darf, wohingegen keinerlei Aussagen über

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

die Zulässigkeit der Verarbeitung nach anderen Bestimmungen getätigt werden. Nach § 102a Abs 1 gespeicherte Daten könnten demnach für die Zwecke der § 53 Abs 3a SPG, § 22 Abs 2a Militärbefugnisgesetz (MBG) oder § 87b Abs 3 UrhG verarbeitet werden. Aus den im Folgenden dargestellten Gründen sollte auch eine Verarbeitung der Daten nur unter den Voraussetzungen der StPO möglich sein.

§ 53 Abs 3a Satz 1 SPG sieht ebenso wie § 22 Abs 2a MBG vor, dass von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Namen, Anschrift und Teilnehmernummer eines „bestimmten" Anschlusses verlangt werden können. Eine solche „Bestimmung" eines Anschlusses wäre wohl auch durch die Angabe eines konkreten Zeitpunktes in der Vergangenheit möglich, in dem dem Anschluss eine bestimmte IP-Adresse zugewiesen war. Diesfalls käme es zu einer Verarbeitung der nach § 102a Abs 1 gespeicherten Daten. Die Problematik liegt hierbei darin, dass eine Verarbeitung von nach § 102a Abs 1 gespeicherten Daten zu dem Zweck der Ermittlung eines durch die Angaben der Behörden „bestimmten" Anschlusses ein außerordentlich großes Eingriffspotential aufweist. Denn bereits eine geringfügige Ausweitung der derzeit nach SPG bzw. MBG bestehenden Befugnisse würde technische Verfahren ähnlich einem Data Mining ermöglichen. So sieht § 53 Abs 3a Satz 2 SPG bereits für den Bereich der Telefonie (arg „Gespräch") vor, dass für die Erfüllung bestimmter Aufgaben die „Bestimmung" des Anschlusses auch durch Bezeichnung des Zeitpunktes des Gesprächs und der passiven Teilnehmernummer erfolgen kann. Wäre die Bestimmung des Anschlusses auch durch die Angabe bestimmter Aufenthaltsorte (d.h. Cell-IDs) oder Kommunikationspartner (ohne zeitliche Präzisierung) möglich, so würde eine derartige Datenverarbeitung eine Eingriffsintensität entwickeln, die einem automationsunterstützten Datenabgleich (§ 149i StPO; „Rasterfahndung") nahe kommt. Der technische Unterschied zwischen einem Data Mining in der hier beschriebenen Art und einer Rasterfahndung besteht nur insofern, dass im Rahmen einer Rasterfahndung mehrere (grundsätzlich kleinere) Datenbestände vereint werden, wohingegen bei einem Data Mining bereits ein zentraler Datenbestand von außerordentlicher Größe besteht. Die Tatsache, dass das Data Mining nicht von einer Behörde, sondern in ihrem Auftrag von einem privaten Unternehmen durchgeführt wird,

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

mindert keinesfalls das Ausmaß des Eingriffs in die Grundrechte der Betroffenen.

Darüber hinaus ist der nach den Bestimmungen des SPG oder MBG bestehende Rechtsschutz gänzlich unzureichend ausgestaltet. § 91a Abs 3 SPG normiert unter welchen Voraussetzungen die Sicherheitsbehörden die Zustimmung des nach § 91a SPG eingerichtete Rechtsschutzbeauftragten einzuholen haben. Eine solche Zustimmung ist erforderlich, wenn sich „eine Aufgabe gemäß § 21 Abs 3 [SPG] stellt“ oder beabsichtigt ist, im Rahmen der erweiterten Gefahrenerforschung (§ 21 Abs 3 SPG) besondere Ermittlungsmaßnahmen nach § 54 Abs 3 und 4 SPG zu setzen oder gemäß § 53 Abs 5 SPG ermittelte Daten weiterzuverarbeiten“. Aus einem Umkehrschluss ergibt sich daher, dass zur Ausübung der Befugnisse nach § 53 Abs 3a SPG keine Zustimmung des Rechtsschutzbeauftragten erforderlich ist. Gemäß § 91c Abs 1 SPG besteht auch keine Pflicht den Rechtsschutzbeauftragten über die Ausübung der Befugnisse gemäß § 53 Abs 3a zu informieren. Für den Bereich des MBG gilt, dass gemäß § 57 Abs 1 MBG ein Rechtsschutzbeauftragter einzurichten ist, dessen Aufgabe ua die Prüfung der Rechtmäßigkeit von Maßnahmen der nachrichtendienstlichen Abwehr ist. § 57 Abs 3 MBG normiert umfassende Auskunftspflichten der militärischer Organe und Dienststellen gegenüber dem Rechtsschutzbeauftragten. Diese Auskunftspflichten sind jedoch entscheidend dadurch beschränkt, dass sie gemäß § 57 Abs 4 Satz 3 MBG nicht gelten „für Auskünfte und Unterlagen über die Identität von Personen oder über Quellen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde, und für Abschriften und Kopien, wenn das Bekanntwerden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde“.

Weiters bestehen gemäß Art 52 Abs 2 Satz 2 B-VG die Auskunftspflichten gegenüber den ständigen Unterausschüssen des Nationalrats nicht betreffend „Auskünfte und Unterlagen, insbesondere über Quellen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde“. Da stets jene Behörde, die die Befugnis nach § 22 Abs 2a MBG ausübt (bzw. der Bundesminister für Landesverteidigung), festzustellen hat, ob die „nationale Sicherheit“ gefährdet ist, können die bestehenden Aufsichts- und

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Kontrollrechte allzu leicht ausgehebelt werden.

Ähnlich wie § 53 Abs 3a Satz 1 SPG oder § 22 Abs 2a MBG sieht auch § 87b Abs 3 UrhG vor, dass unter bestimmten Umständen Auskunft über Name und Anschrift eines Anschlussinhabers erteilt werden muss. Dieser zivilrechtliche Auskunftsanspruch steht Rechteinhabern zu, deren Ausschließungsrechte nach dem UrhG verletzt wurden. Anspruchsgegner sind Vermittler iSd § 81 Abs 1a UrhG, worunter insbesondere auch Access Provider zu subsumieren sind, die gemäß § 102a Abs 1 zur Vorratsspeicherung verpflichtet sind. Da nur im Streitfall über das Bestehen eines Auskunftsanspruchs ein ordentliches Gericht über eine auf § 87b Abs 3 UrhG gegründete Datenverarbeitung entscheidet, ist diesfalls grundsätzlich keine ex ante erfolgende Kontrolle der Verarbeitung von gemäß § 102a Abs 1 gespeicherter Daten gegeben. Der im Fall des § 87b Abs 3 UrhG gegebene Rechtsschutz für Betroffene ist daher als gänzlich unzulänglich zu beurteilen.

Aus den obigen Ausführungen ergibt sich die Notwendigkeit nicht nur die Übermittlung, sondern auch die Verarbeitung der gemäß § 102a Abs 1 gespeicherten Daten nur unter den Voraussetzungen der StPO zu ermöglichen, somit ausnahmslos einen Richtervorbehalt vorzusehen.

Der denkbaren Forderung nach einer Datenübermittlung oder -verarbeitung ohne die Erforderlichkeit eines Gerichtsbeschlusses, die mit dem Argument gestützt werden könnte, dass die Daten „ohnedies gespeichert würden“, soll an dieser Stelle entgegen getreten werden. Bei dieser Forderung würde es sich um einen naturalistischen Fehlschluss handeln, da von der Möglichkeit der Datenverarbeitung (einem Sein) darauf geschlossen wird, dass diese Datenverarbeitung rechtlich zulässig sein soll.

Aus den oben dargestellten Gründen sollte auch eine Verarbeitung der Daten nur unter den Voraussetzungen der StPO zulässig sein. Es wird daher empfohlen, in § 102a Abs 1 die Textstelle *„zum Zweck der Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17 SPG), einschließlich der Tatbestände der §§ 107 und*

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

107a StGB" zu streichen und folgenden Text als zweiten Satz des § 102a Abs 1 einzufügen: *„Die Verwendung (§ 4 Z 20 DSG 2000) dieser Daten hat ausschließlich zu dem Zweck der Erfüllung der nach der StPO iVm § 94 Abs 2 bestehenden Mitwirkungspflichten zu erfolgen."*

Ein expliziter Verweis auf § 149b StPO sollte nicht aufgenommen werden, um keine Novellierung bei Inkrafttreten des § 135 StPO idF BGBl I Nr 19/2004 erforderlich zu machen.

Die in § 149a Abs 2 StPO bzw. § 135 Abs 2 StPO idF BGBl I Nr 19/2004 vorgenommene Differenzierung je nach Vorliegen einer Zustimmung des Anschlussinhabers erscheint nicht nur zweckmäßig, sondern auch verfassungsrechtlich geboten.

Bezüglich der Erforderlichkeit der Novellierung des § 149a Abs 2 StPO bzw. § 135 Abs 2 StPO idF BGBl I Nr 19/2004 siehe unten.

5. Zu § 102a Abs 4

§ 102a Abs 4 verweist bezüglich der Zuständigkeit der Datenschutzkommission (DSK) auf § 114 TKG 2003. Hierbei handelt es sich offenbar um einen Redaktionsfehler, da § 114 TKG 2003 nicht geeignet ist eine Zuständigkeit der DSK zu begründen. Gewollt war wohl ein Verweis auf den neu eingefügten § 114a.

6. Zu § 102b

§ 102b normiert Auskunftspflichten von Anbietern und Betreibern öffentlicher Kommunikationsnetze gegenüber dem Bundesminister für Justiz. Nach dem vorliegenden Entwurf beschränken sich diese Auskunftspflichten auf „im Einklang mit den Bestimmungen der StPO" weitergegebene Daten. Eine derartige Einschränkung ist entschieden abzulehnen, da gerade in jenen Fällen ein besonderer Bedarf an Transparenz besteht, in denen unter

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Verletzung der Bestimmungen der StPO Daten weitergegeben worden sind. Die Frage, ob die Daten an die zuständige Behörde weitergegeben wurden, ist daher ebenso irrelevant.

Daher wird vorgeschlagen, dass § 102b Z 1 wie folgt gefasst wird: *„in welchen Fällen Daten weitergegeben worden sind“*. § 102b Z 2 sollte lauten: *„wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie angefordert wurden, vergangen ist“*.

Weiters ist zu betonen, dass die Erfüllung der vorgesehenen Auskunftspflichten für Anbieter und Betreiber einen Eingriff in das Grundrecht auf Erwerbsfreiheit gemäß Art 6 StGG und in das Grundrecht auf Eigentum gemäß Art 5 StGG und Art 1 1. ZPEMRK darstellt. Das öffentliche Interesse, das geeignet sein könnte diesen Eingriff zu rechtfertigen, liegt insbesondere darin, dass mit der Auskunftspflicht über die Überwachungsmaßnahmen ein gewisses Maß an Transparenz des Regimes der Vorratsdatenspeicherung herbeigeführt wird. Die Eignung der Auskunftspflicht zur Erreichung dieses Zweckes ist gegeben. Die Erforderlichkeit die Auskunftspflicht Anbietern und Betreibern (dh Privaten) und nicht den die Überwachungsmaßnahmen anordnenden Behörden aufzuerlegen, ergibt sich daraus, dass die gewünschte Transparenz auf diese Weise wesentlich besser gewährleistet werden kann.

Wie unter II.10. noch näher ausgeführt wird, ist eine Kostenregelung unter Beachtung des Sachlichkeitsgebots und des Verhältnismäßigkeitsgrundsatzes erforderlich (vgl. VfSlg 16.808/2003), widrigen Falls § 102b uE als verfassungswidrig zu beurteilen wäre.

7. Zu § 114a

§ 114a begründet eine Zuständigkeit der Datenschutzkommission (DSK) „nach Maßgabe des § 1 Abs 5 letzter Satz DSG 2000“. Gemäß § 1 Abs 5 lt Satz DSG 2000 besteht aber insbesondere dann keine Zuständigkeit der DSK, wenn Akte der Gerichtsbarkeit betroffen

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

sind. Da die Anbieter und Betreiber bei einer Datenübermittlung aufgrund eines richterlichen Beschlusses als Inpflichtgenommene der Gerichte tätig werden und insofern ein Akt der Gerichtsbarkeit vorliegt, würde für diesen wichtigen Bereich entgegen der Formulierung in § 102a Abs 4 eigentlich keine Zuständigkeit der DSK bestehen. Es wird daher empfohlen, den Verweis auf § 1 Abs 5 DSG 2000 zu streichen.

8. Zu § 137 Abs 2

Die in § 137 Abs 2 normierte Legisvakanz sollte sich nicht auf § 114 TKG 2003, sondern auf den neu eingefügten § 114a beziehen, sofern wie oben (unter 5.) gezeigt, ein Redaktionsfehler vorliegt.

9. Zu § 149a StPO und § 135 StPO idF BGBl I Nr 19/2004

§ 149a StPO als auch § 135 StPO idF BGBl I Nr 19/2004 sind in geltender Fassung bereits auch auf eine Überwachung anwendbar, die sich auf einen vergangenen Zeitraum bezieht. Die Voraussetzungen unter denen eine solche Überwachung in Bezug auf einen vergangenen Zeitraum ermöglicht werden soll, sind im Vergleich zu auf die Zukunft gerichtete Überwachungen zu verschärfen.

Allgemein gilt, dass mit der Höhe der Strafdrohung das öffentliche Interesse an der Aufklärung einer bestimmten strafbaren Handlung steigt. Ein öffentliches Interesse, das geeignet sein soll einen Grundrechtseingriff zu rechtfertigen, muss daher umso größer sein, je schwerer der Grundrechtseingriff ist. Eine auf die Zukunft gerichtete Speicherung von personenbezogenen Daten bei Vorliegen eines konkreten Verdachts ist im Verhältnis zu einer flächendeckenden verdachtsunabhängigen Speicherung von Daten „auf Vorrat“ ein vergleichsweise leichter Grundrechtseingriff. Ein öffentliches Interesse, das geeignet ist eine flächendeckende verdachtsunabhängige Vorratsspeicherung rechtfertigen zu können, muss

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

daher größer sein als jenes öffentliche Interesse, dass eine auf die Zukunft gerichtete Überwachung zu rechtfertigen vermag. Hieraus ergibt sich, dass insbesondere bei Fehlen der Zustimmung des Anschlussinhabers eine auf die Vergangenheit gerichtete Überwachung nur unter schwereren Voraussetzungen verfassungsrechtlich zulässig sein kann, als dies derzeit § 149a Abs 2 Z 2 StPO bzw. § 135 Abs 2 Z 3 StPO idF BGBl I Nr 19/2004 vorsieht. Es wird daher nachdrücklich empfohlen, § 149a Abs 2 Z 2 StPO wie folgt zu fassen:

„in den Fällen des Abs. 1 Z 1 lit. a und b auch, wenn zu erwarten ist, dass dadurch im Fall einer auch einen vergangenen Zeitraum betreffenden Überwachung die Aufklärung eines Verbrechens (§ 17 Abs 1 StGB), ansonsten die Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung gefördert werden kann und durch die Überwachung Daten des Verdächtigen ermittelt werden können,“

Dem entsprechend sollte § 135 Abs 2 Z 3 StPO idF BGBl I Nr 19/2004 wie folgt lauten:

„wenn zu erwarten ist, dass dadurch im Fall einer auch einen vergangenen Zeitraum betreffenden Überwachung die Aufklärung eines Verbrechens (§ 17 Abs 1 StGB), ansonsten die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.“

Hierdurch werden zweifelsfrei jene Delikte, die Anlass für die Erlassung der DR-RL waren, erfasst. Hierzu zählen insbesondere die Anführung einer terroristischen Vereinigung (§ 278b Abs 1 StGB), die Beteiligung als Mitglied in einer terroristischen Vereinigung (§ 278b Abs 2 StGB) sowie die Gründung einer bzw. die Beteiligung an einer kriminellen Organisation (§ 278a StGB).

Entsprechend der Erhöhung jener Strafdrohung, die für eine Überwachung ohne Zustimmung des Anschlussinhabers erforderlich ist, sollte aus denselben Gründen für Überwachungen, die auch auf die Vergangenheit gerichtet sind, ebenfalls eine erhöhte

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Strafdrohung erforderlich sein. Eine Verdopplung der erforderlichen Strafdrohung von einer mehr als sechsmonatigen zu einer mehr als einjährigen Freiheitsstrafe erscheint hierbei geboten. Es wird daher empfohlen § 149a Abs 2 Z 1 StPO wie folgt zu fassen:

„wenn zu erwarten ist, dass dadurch im Fall einer auch einen vergangenen Zeitraum betreffenden Überwachung die Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung, ansonsten die Aufklärung einer vorsätzlich begangenen, mit mehr als sechsmonatiger Freiheitsstrafe bedrohten strafbaren Handlung gefördert werden kann und der Inhaber des Teilnehmeranschlusses der Überwachung ausdrücklich zustimmt,“

Derselben Wertung entsprechend sollte § 135 Abs 2 Z 2 StPO idF BGBl I Nr 19/2004 wie folgt lauten:

„wenn zu erwarten ist, dass dadurch im Fall einer auch einen vergangenen Zeitraum betreffenden Überwachung die Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung, ansonsten die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder“

10. Zur fehlenden Regelung über die Kostentragung

Die DR-RL enthält keine Regelungen über die Tragung der durch die Vorratsspeicherung entstehenden Kosten. Es ist daher jedem Mitgliedstaat überlassen, für diese Frage eine Regelung zu treffen.

Die Erläuterungen führen aus, dass die Speicherpflicht gemäß § 102a „ausschließlich Daten

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

betrifft, die bereits derzeit für Verrechnungszwecke gespeichert werden“. Dies ist nicht zutreffend. Derzeit darf die Standortkennung (Cell-ID) nicht gespeichert werden, da diese für die Zwecke der Verrechnung nicht erforderlich ist. Selbiges gilt für die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigten Daten betreffend Internetzugang und Internet-E-Mail – mit Ausnahme der Speicherung der vergebenen statischen IP-Adressen. Es ist daher nicht zutreffend, dass Mehrkosten „lediglich daraus entstehen, dass einerseits die Speicherung nunmehr anders strukturiert wird […] und andererseits durch die Befolgung der Anordnungen selbst“. Insofern erfolgt zweifellos ein Eingriff in das gemäß Art 5 StGG und Art 1 1. ZP-MRK geschützte Grundrecht auf Eigentum.

Insbesondere die initiale Einführung entsprechender Überwachungs- und Speicheranlagen wird abhängig von der Größe des Providers mit erheblichen Kosten verbunden sein. Ein großer Teil dieser Kosten entsteht alleine aufgrund der erforderlichen Anpassung von nach einschlägigen Sicherheitsstandards zertifizierten innerbetrieblichen Prozessen. Dies trifft insbesondere auf Internet Service Provider zu, da diese derzeit keine Standort- und abgesehen von statischen IP-Adressen auch keine Verkehrsdaten speichern. Da bezüglich Organisation und Prozess-Management bei jeder Änderung der Überwachungs- und Speichereinrichtungen erneut erhebliche Kosten entstehen, ist auch aus diesem Grund die derzeit vorgesehene schrittweise Einführung von Speicherpflichten im Bereich des Internets abzulehnen.

Da entgegen den in den Erläuterungen enthaltenen Aussagen durch die Erfüllung der Pflicht zur Speicherung der in § 92 Abs 3 Z 4b genannten Daten Mehrkosten entstehen, ist eine Kostenregelung unter Beachtung des Verhältnismäßigkeitsgrundsatzes erforderlich (vgl. VfSlg 16.808/2003). Die Tatsache, dass offenbar keine amtlichen Erhebungen der für die Datenspeicherung den privaten Betreibern erwachsenden Kosten durchgeführt wurden, kann ebenso wenig wie allfällige budgetäre Gründe als sachliche Rechtfertigung für eine gänzliche Kostentragung durch die privaten Betreiber dienen.

Mangels einer den Verhältnismäßigkeitsgrundsatz beachtenden Kostentragung ist die in

e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

§ 102a vorgesehene Speicherpflicht daher als verfassungswidrig zu beurteilen. Eine § 94 Abs 2 TKG 2003 entsprechende gesetzliche Regelung erscheint daher verfassungsrechtlich geboten. § 102a sollte daher um einen Abs 5 erweitert werden:

„Der Bundesminister für Justiz hat im Einvernehmen mit dem Bundesminister für Verkehr, Innovation und Technologie, dem Bundesminister für Finanzen, dem Bundesminister für Inneres und dem Bundesminister für Landesverteidigung durch Verordnung einen angemessenen Kostenersatz vorzusehen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, Bedacht zu nehmen."

III. Zusammenfassung der Änderungsvorschläge

Im Folgenden findet sich eine Zusammenfassung aller zuvor erörterten Änderungsvorschläge. Zu streichende Textpassagen sind durchgestrichen worden, wohingegen hinzugefügte Passagen durch Unterstreichung gekennzeichnet wurden.

TKG 2003

1a. § 90 Abs 6 lautet:

(6) Betreiber von Kommunikationsdiensten sind verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten im Sinne von § 92 Abs. 3 Z 3 ~~lit. a bis e~~ lit. a bis d von Teilnehmern zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben.

4. § 92 Abs. 3 Z 3 lautet:

„3. „Stammdaten" alle personenbezogenen Daten, die für die Begründung, die Abwicklung,

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

„a) ~~Daten gemäß Z 4a lit. a; dabei bezeichnet der Begriff~~

~~aa) „Name“ Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen,~~

~~bb) „Anschrift“ Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen,~~

Name und Anschrift

b) akademischer Grad bei natürlichen Personen,

c) Information über Art und Inhalt des Vertragsverhältnisses,

d) ~~Bonität;~~ Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,

e) Bonität;“

5. ~~In § 92 Abs. 4a lautet~~ Nach § 92 Abs 3 Z 4a wird nachstehende Z 4b eingefügt:

„~~4a~~ 4b. „Vorratsdaten“ jene Stamm-, Verkehrs- und Standortdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs erzeugt oder verarbeitet werden, einschließlich der Daten erfolgloser Anrufversuche, soweit diese Daten anlässlich der Erbringung von Telefondiensten gespeichert oder anlässlich der Erbringung von Internetdiensten protokolliert werden; dies sind:

a) zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten:

aa) betreffend Telefonfestnetz und Mobilfunk:

- die Rufnummer des anrufenden Anschlusses,
- der Name und die Anschrift des Teilnehmers oder registrierten Benutzers;

~~bb) betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:~~

~~- die zugewiesene(n) Benutzerkennung(en),~~

~~- die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden,~~

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

(e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

~~- der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Internetprotokoll- Adresse (IP-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;~~

b) zur Identifizierung des Adressaten einer Nachricht benötigte Daten betreffend Telefonfestnetz
und Mobilfunk:

- die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird,
- die Namen und Anschriften der Teilnehmer oder registrierten Benutzer;

c) zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:

- betreffend Telefonfestnetz und Mobilfunk: Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs;

d) zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:

- betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;

e) zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:

aa) betreffend Telefonfestnetz: die Rufnummern des anrufenden und des angerufenen Anschlusses;

bb) betreffend Mobilfunk:

- die Rufnummern des anrufenden und des angerufenen Anschlusses,
- die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses,
- die internationale Mobilfunkgerätekennung (IMEI) des anrufenden Anschlusses,
- die IMSI des angerufenen Anschlusses,
- die IMEI des angerufenen Anschlusses,

~~cc)~~ - im Falle vorbezahlter anonymer Dienste: Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde;

(e making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

f) zur Bestimmung des Standorts mobiler Geräte benötigte Daten:

- die Standortkennung (Cell-ID) bei Beginn der Verbindung,
- Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt."

5a. Nach § 92 Abs 3 Z 10 werden die nachstehende Ziffern 11 und 12 eingefügt:

11. „Name" Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen;

12. „Anschrift" Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen.

7. Nach § 102 wird nachstehender § 102a samt Überschrift eingefügt:

„Speicherung von Vorratsdaten

§ 102a. (1) Abweichend von den §§ 96, 99 und 102 haben Anbieter und Betreiber öffentlicher

Kommunikationsnetze die in § 92 Abs. 3 ~~Z 4a~~ Z 4b aufgezählten Daten, soweit diese im Zuge der Bereitstellung des Kommunikationsdienstes erzeugt oder verarbeitet werden, für einen Zeitraum von sechs Monaten ab dem Zeitpunkt der Beendigung des Kommunikationsvorganges ~~zum Zweck der Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17 SPG), einschließlich der Tatbestände der §§ 107 und 107a StGB~~ zu speichern. Die Verwendung (§ 4 Z 20 DSG 2000) dieser Daten hat ausschließlich zu dem Zweck der Erfüllung der nach der StPO iVm § 94 Abs 2 bestehenden Mitwirkungspflichten zu erfolgen. Die Daten sind nach Ablauf dieser Frist, unbeschadet des § 99 Abs. 2, unverzüglich zu löschen.

(2) Die Daten sind so zu speichern, dass sie und alle sonstigen damit zusammenhängenden erforderlichen Informationen unverzüglich an die für die Durchführung einer Überwachung einer Telekommunikation zuständigen Behörden auf Grund einer gerichtlichen Anordnung oder Bewilligung weitergeleitet werden können.

(3) Die Daten gemäß Abs. 1 sind von der gleichen Qualität und unterliegen der gleichen

palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten. Die Daten gemäß Abs. 1 sind durch geeignete technische und organisatorische Maßnahmen gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust sowie zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen. Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist.

(4) Die Anbieter und Betreiber öffentlicher Kommunikationsnetze gewährleisten, dass jede Anfrage und jede Übermittlung von Daten nach dieser Bestimmung protokolliert wird. Diese Protokollierung umfasst folgende Angaben:

1. die übermittelten Datenarten,
2. das Datum und den genauen Zeitpunkt der Übermittlung,
3. eine Referenz zu der gerichtlichen Anordnung gemäß § 149b StPO, die der Übermittlung der Daten zugrunde liegt.

Die Anbieter und Betreiber öffentlicher Kommunikationsnetze teilen die Protokolldaten der für die Datenschutzkontrolle gemäß § 114 zuständigen Datenschutzkommission auf Ersuchen unverzüglich mit. Protokolldaten dürfen ausschließlich für die Zwecke der Kontrolle des Datenschutzes durch die Datenschutzkommission und zur Gewährleistung der Datensicherheit verwendet werden.

(5) Der Bundesminister für Justiz hat im Einvernehmen mit dem Bundesminister für Verkehr, Innovation und Technologie, dem Bundesminister für Finanzen, dem Bundesminister für Inneres und dem Bundesminister für Landesverteidigung durch Verordnung einen angemessenen Kostenersatz vorzusehen. Dabei ist insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, Bedacht zu nehmen.“

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

8. Nach § 102a wird nachstehender § 102b samt Überschrift eingefügt:

„Auskunftspflichten

§ 102b. Anbieter und Betreiber öffentlicher Kommunikationsnetze sind verpflichtet, dem Bundesminister für Justiz auf schriftliches Verlangen die Auskünfte zu erteilen, die für den Vollzug von § 102a und der jährlichen Berichterstattung gegenüber der Europäischen Kommission notwendig sind. Dies sind insbesondere Auskünfte darüber

1. in welchen Fällen ~~im Einklang mit den Bestimmungen der StPO~~ Daten ~~an die zuständigen Behörden~~ weitergegeben worden sind;
2. wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie ~~von den zuständigen Behörden nach den Bestimmungen der StPO~~ angefordert wurden, vergangen ist;
3. in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind.“

„Kontrolle durch die Datenschutzkommission

§ 114a. Die Datenschutzkommission kontrolliert die Vollziehung von § 102a ~~nach Maßgabe des § 1 Abs. 5 letzter Satz DSG 2000~~.“

13. Der bisherige § 137 wird als Abs. 1 bezeichnet und folgender Abs. 2 angefügt:

„(2) §§ 1, 92, 102a, 102b, 103, 109 und ~~114~~ 114a in der Fassung des Bundesgesetzes BGBl. I

Nr. XX/2007 treten mit 1. September 2007 in Kraft.“

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

StPO geltende Fassung

V. Überwachung einer Telekommunikation

§ 149a StPO. (2) Die Überwachung einer Telekommunikation ist zulässig,

1. wenn zu erwarten ist, dass dadurch im Fall einer auch einen vergangenen Zeitraum betreffenden Überwachung die Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung, ansonsten die Aufklärung einer vorsätzlich begangenen, mit mehr als sechsmonatiger Freiheitsstrafe bedrohten strafbaren Handlung gefördert werden kann und der Inhaber des Teilnehmeranschlusses der Überwachung ausdrücklich zustimmt,
2. in den Fällen des Abs. 1 Z 1 lit. a und b auch, wenn zu erwarten ist, dass dadurch im Fall einer auch einen vergangenen Zeitraum betreffenden Überwachung die Aufklärung eines Verbrechens (§ 17 Abs 1 StGB), ansonsten die Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung gefördert werden kann und durch die Überwachung Daten des Verdächtigen ermittelt werden können,
3. in den Fällen des Abs. 1 Z 1 lit. c auch, wenn die Überwachung zur Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung erforderlich erscheint und
   a) der Inhaber des Teilnehmeranschlusses selbst dringend verdächtig ist, die Tat begangen zu haben, oder
   b) Gründe für die Annahme vorliegen, dass eine der Tat dringend verdächtige Person den Teilnehmeranschluss benützen oder eine Verbindung mit ihm herstellen werde.

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu

e-center
vienna | brussels | london | leipzig | prague | budapest
europäisches zentrum für e-commerce und internetrecht
european center for e-commerce and internet law

leitung:
ao. univ.-prof. dr. wolfgang zankl
rechtsträger:
juranovit forschungs gmbh
partner:
auditor-deloitte
atv
emc²
erste bank
first data
gassauer-fleissner
hutchison 3g
mbo-media
microsoft
mobilkom austria
one
siemens
telekom austria
tele.ring
t-mobile
wiener wirtschaftsförderungsfonds
wolf theiss

StPO idF BGBl I Nr 19/2004

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung sowie Überwachung von Nachrichten

§ 135. (2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,
2. wenn zu erwarten ist, dass dadurch im Fall einer auch einen vergangenen Zeitraum betreffenden Überwachung die Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung, ansonsten die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder
3. wenn zu erwarten ist, dass dadurch im Fall einer auch einen vergangenen Zeitraum betreffenden Überwachung die Aufklärung eines Verbrechens (§ 17 Abs 1 StGB), ansonsten die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

making it legal
palais esterhazy
wallnerstraße 4
1010 wien
tel: +43 1 5354660
fax: +43 1 5354660 490
www.e-center.eu
office@e-center.eu