REPUBLIK ÖSTERREICH
DATENSCHUTZKOMMISSION

A-1010 Wien, Ballhausplatz 1
Tel. ++43-1-531 15/0
Fax: ++43-1-531 15/2690
e-mail: dsk@dsk.gv.at
DVR: 0000027

Sachbearbeiter: Mag. Marcus Hild LL.M., Klappe 2887
E-Mails in dieser Sache bitte an: dsk@dsk.gv.at
Faxsendungen bitte nur an die oben angegebene Nummer!

GZ: K213.000/0005-DSK/2006

Verfahren nach § 30 DSG 2000,
Speicherung von dynamisch vergebenen
IP Adressen

Empfehlung der DSK

Anonymisierte Fassung

E M P F E H L U N G

Die Datenschutzkommission hat unter dem Vorsitz von Dr. SPENLING und in Anwesenheit der Mitglieder Mag. HUTTERER, Dr. KOTSCHY, Dr. HEISSENBERGER, Dr. PREISS und Dr. ROSENMAYR-KLEMENZ sowie des Schriftführers Mag. SUDA in ihrer Sitzung vom 29. September 2006 folgenden Beschluss gefasst:

Auf Grund des im amtswegigen Verfahren ermittelten und unter Berücksichtigung auch der Stellungnahme der N*** Internet Service Provider GmbH (in der Folge als „N*** ISP GmbH“ bezeichnet) festgestellten Sachverhalts, ergeht gemäß § 30 Abs 6 des Datenschutzgesetzes 2000 (DSG 2000) BGBl. I Nr.165/1999 idF BGBl. I Nr. 13/2005 die folgende Empfehlung:

Die N*** ISP GmbH möge innerhalb einer Frist von vier Wochen ab Zustellung dieser Empfehlung Vorsorge dafür treffen, dass in Hinkunft dynamisch vergebene IP Adressen nach Abschluss der technischen und organisatorischen Abwicklung der Verbindung ohne Zustimmung des Benutzers nicht mehr gespeichert werden.

B e g r ü n d u n g :

Aufgrund der Eingaben zweier Betroffener, die einer Gesellschaft, die die Wahrnehmung von Leistungsschutzrechten zum Unternehmensgegenstand hat, vorwarfen, personenbezogene Daten missbräuchlich unter Verletzung des Telekommunikationsgeheimnisses zu ermitteln und zu verarbeiten, ist bei der DSK der begründete Verdacht entstanden, dass

Verkehrsdaten im Sinne von § 92 Abs 3 Z 4 TKG 2003 entgegen den Bestimmungen des TKG 2003 verwendet werden. Die Datenschutzkommission hat daher die Verwendung von Verkehrsdaten durch die N*** ISP GmbH gemäß § 30 Abs 2 DSG 2000 überprüft.

Der Access-Provider der beiden Betroffenen, die N*** ISP GmbH, führte zur Frage, welcher Natur die von ihm vergebenen IP-Adressen gewesen seien, aus, dass die an die beiden Betroffenen vergebenen Adressen dynamische IP-Adressen waren. Zur Frage, wieso er die in Rede stehenden Verkehrsdaten (IP-Adressen) zum Zeitpunkt der gerichtlichen Anforderung noch gespeichert hatte, erklärte er, dass er zwar ein flat-rate Verrechnungssystem habe, jedoch die IP-Adressen zum Zweck der Überprüfung der Einhaltung der Fair Use Policy speichern müsse.

Aufgrund der nicht miteinander in Widerspruch stehenden Angaben der beiden Betroffenen sowie aufgrund der Ausführungen der zur Stellungnahme aufgeforderten Leistungsverwertungsgesellschaft sowie der N*** ISP GmbH wurde folgender Sachverhalt festgestellt:

Die Leistungsverwertungsgesellschaft hat durch regelmäßiges Aufsuchen von Filesharing-Systemen im Internet, die mit Hilfe spezieller Programme angesteuert werden können, und im Prinzip jedermann zugänglich sind, auch von den Rechnern der beiden Betroffenen gemachte Angebote aufgefunden, mit denen unter Verstoß gegen § 86 Abs 1 Z 2 bis 4 UrhG Musikstücke zum Download zur Verfügung gestellt wurden. Da diese Kommunikation in Form einer direkten Peer-to-Peer (P2P) Verbindung stattfand, war die jeweils vom anbietenden Rechner (das sind die Geräte der beiden Betroffenen) im relevanten Zeitpunkt verwendete IP-Adresse für den anderen Kommunikationsteilnehmer (den Beauftragten der Leistungsverwertungsgesellschaft) ersichtlich.
Als Ergebnis dieser Kommunikationen wurden vom Beauftragten der Leistungsverwertungsgesellschaft folgende Daten ermittelt: Die IP-Adressen der anbietenden Anschlüsse, der Zeitpunkt der Kommunikation sowie die Menge der zum Herunterladen angebotenen Musiktitel.

Daraufhin beantragte die Leistungsverwertungsgesellschaft beim Landesgericht für Strafsachen Wien, Vorerhebungen gegen unbekannte Täter wegen des Verdachts des Vergehens nach § 91 Abs 1 UrhG einzuleiten. Beantragt werde, das Gericht möge den Beschluss fassen, die N*** ISP GmbH möge bekannt geben, wer am 17.8.2004 zwischen 9:47:18 und 10:15:05 Uhr eine bestimmte IP-Adresse verwendet habe und wer am 31.8.2004 zwischen 4:36:40 und 5:21:50 Uhr eine bestimmte IP-Adresse verwendet habe.

Diesen Anträgen ist das Gericht nachgekommen, einerseits mit einem ausdrücklich auf die „§§ 7 ff DSG“ gestützten Beschluss vom 19. November 2004 „wegen § 91 UrhG“ und andererseits mit einem auf § 96 Abs 7 TKG iVm §§ 86ff UrhG gestützten Beschluss vom 29. November 2004.

Daraufhin gab am 23. Dez. 2004 die N*** ISP GmbH dem LG für Strafsachen Wien bekannt, dass die mitgeteilte IP-Adresse zum angegebenen Zeitpunkt einer Betroffenen zugeteilt war. Als Rechtsgrundlage für diese Mitteilung ist im Fax „§§ 7 ff DSG“ angegeben. Am 14.1.2005 übermittelte die N*** ISP GmbH Name und Anschrift der zweiten Betroffenen an die vom Gericht ersuchte Kriminaldirektion 1 der Bundespolizeidirektion Wien.

Ergänzend führt die Leistungsverwertungsgesellschaft in ihren Stellungnahmen gegenüber der Datenschutzkommission – offenbar im Hinblick auf ihre eigene Verarbeitung fremder IP-Adressen für Zwecke der Rechtsverfolgung – aus, dass nach ihrer Ansicht dynamische IP-Adressen keine personenbezogenen Daten seien und daher Datenschutzrelevanz der gegenständlichen Verarbeitungsschritte erst ab dem Stadium des Datenabgleichs beim Access-Provider zum Zweck der Identitätsermittlung des Teilnehmers gegeben sei.

R e c h t l i c h e E r w ä g u n g e n :

1. Angewendete Rechtsvorschriften:

§ 92 Abs 3 TKG 2003 lautet in der geltenden Fassung:

„(3) In diesem Abschnitt bezeichnet unbeschadet des § 3 der Begriff
1. „Anbieter“ Betreiber von öffentlichen Kommunikationsdiensten;
2. „Benutzer“ eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;
3. „Stammdaten“ 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; dies sind:
a) Familienname und Vorname,
b) akademischer Grad,
c) Wohnadresse,
d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
e) Information über Art und Inhalt des Vertragsverhältnisses,
f) Bonität;
4. „Verkehrsdaten“ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;
4a. „Zugangsdaten“ 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;
5. „Inhaltsdaten“ die Inhalte übertragener Nachrichten (Z 7);
6. „Standortdaten“ Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben;
[…….]“

§ 93 TKG 2003 lautet in der geltenden Fassung:

„Kommunikationsgeheimnis

§ 93. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.
(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.
(4) Werden mittels einer Funkanlage, einer Telekommunikationsendeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Telekommunikationsendeinrichtung oder den Anwender der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke.“

§ 99 TKG 2003 lautet in der geltenden Fassung:

„Verkehrsdaten

§ 99. (1) Verkehrsdaten dürfen außer in den gesetzlich geregelten Fällen nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren.
(2) Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden.
Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.
(3) Die Verarbeitung von Verkehrsdaten darf nur durch solche Personen erfolgen, die für die Entgeltverrechnung oder Verkehrsabwicklung, Behebung von Störungen, Kundenanfragen, Betrugsermittlung oder Vermarktung der Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen zuständig sind oder die von diesen Personen beauftragt wurden. Der Umfang der verwendeten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.
(4) Dem Betreiber ist es außer in den gesetzlich besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Betreiber die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden.“

2. Die Datenschutzkommission hat Folgendes erwogen:

a) zur Frage, ob dynamische IP-Adressen personenbezogene Daten sind:

Die von der Leistungsverwertungsgesellschaft ermittelten IP Adressen sowie die Information über den Verwendungszeitpunkt waren – wie gerade der vorliegende Fall zeigt – Daten, die identifizierbar, d.h. in Bezug zu einer bestimmten Person bringbar waren. Daher stellen die

IP-Adressen im vorliegenden Fall „bestimmbare“ Daten iSd § 4 Z 1 DSG 2000 und daher „personenbezogene Daten“ dar .

b) zur Frage der Verarbeitung von Verkehrsdaten bei der Ermittlung der Identität von Teilnehmern

- Im Anlassfall hat die Befassung jenes Betreibers, der – wie aus der IP-Adresse ersichtlich – die IP-Adresse vergeben hatte, ergeben, dass es sich um eine **dynamische IP-Adresse** handelte. In diesem Fall kann die Identität des Anschlussinhabers nur in mehreren Schritten geklärt werden:
- zunächst muss festgestellt werden, welchem Anschluss zu dem angegebenen Zeitpunkt die angegebene (dynamische) IP-Adresse zugeordnet war;
- erst nachdem der Anschluss so bestimmt wurde, kann die Identität des Teilnehmers, der laut Vertrag mit dem Betreiber Inhaber dieses Anschlusses ist, bestimmt werden.

Daraus folgt, dass bei der gegenständlichen Fragestellung die Heranziehung von Stammdaten zur Identifikation des Anschlussinhabers erst in einem zweiten Schritt erfolgen kann - **als erster Schritt müssen zunächst immer Verkehrsdaten**, nämlich der Zeitpunkt der Verbindung und die benützte dynamische IP-Adresse, **verarbeitet werden**, um die Kennung des Anschlusses zu eruieren:

Wenn der OGH in seiner Entscheidung 11 Os 57/05z vom 26. Juli 2005 ausgesprochen hat, dass die Ermittlung der Identität des Nutzers einer IP-Adresse keine „Feststellung sei, welcher Teilnehmeranschluss Ursprung einer Telekommunikation war“, da die IP-Adresse bereits der „Teilnehmeranschluss“ iSd des § 149a StPO sei, so kann dem für die Frage der Anwendbarkeit des § 149a StPO angesichts des besonderen Schutzzwecks dieser Norm zugestimmt werden. Es ist dem OGH auch zu folgen, wenn er ausführt, dass sich das Auskunftsbegehren an den Access Provider nur auf Stammdaten beziehe, die weder dem Grundrecht des Art. 10a StGG noch dem Kommunikationsgeheimnis des § 93 Abs 1 TKG 2003 unterliegen. Daraus kann jedoch nicht der Schluss gezogen werden, dass für die **Erfüllung des Auskunftsbegehrens** durch Ermittlung der Identität des Inhabers eines Anschlusses bei der Verwendung dynamischer IP-Adressen **keine** Verkehrsdaten verarbeitet werden müssen. Vielmehr muss der Betreiber seine logfiles daraufhin durchsuchen, welchem Anschluss er zu dem angegebenen Zeitpunkt die angegebene IP-Adresse zugeordnet hatte. Dieses Durchsuchen bedingt **beim Betreiber die Verarbeitung von Verkehrsdaten,** da IP-Adressen Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a TKG 2003 und damit Verkehrsdaten im Sinne des § 92 Abs. 3 Z 4 TKG 2003 bzw. des Art. 2 lit b der RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) sind: „Zugangsdaten“ sind 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 (§ 92 Abs 3 Z 4a TKG 2003). IP-Adressen sind solche „Zugangsdaten“ (so auch Einzinger/Schubert/Schwabl/Wessely/Zykan in Medien und Recht 2/05, S 116). Dynamische IP-Adressen sind ausschließlich Verkehrsdaten, statische IP-Adressen sind hingegen sowohl Verkehrsdaten als auch Stammdaten, und zwar letzteres dann, wenn sie angesichts ihrer dauerhaften Vergabe in einem Verzeichnis (vergleichbar einer Telefonnummer) mit den Identitätsdaten eines Teilnehmers verbunden sind.

Die Verwendung von Verkehrsdaten unterliegt der Vertraulichkeit gem. Art 5 der RL 2002/58/EG bzw. dem Kommunikationsgeheimnis gem. § 93 Abs 1 TKG 2003 und besonderen Verwendungsbeschränkungen gem. Art 6 und Art 15 Abs 1 dieser RL bzw. § 92 Abs 2 und § 99 TKG 2003. Diese Verwendungsbeschränkungen bewirken vor allem, dass Verkehrsdaten beim Betreiber über die Herstellung und Aufrechterhaltung der Verbindung im Netz hinaus nur gespeichert bleiben dürfen, soweit dies für Verrechnungszwecke notwendig ist oder soweit die ausdrückliche Einwilligung des Betroffenen vorliegt (Art. 6 der RL 2002/58/EG bzw. § 99 TKG 2003). Darüber hinaus gehende Verwendungen bedürfen einer besonderen gesetzlichen Regelung, die sich im Rahmen des Art 15 Abs 1 der RL halten muss, d.h. nur für einen der in Art. 13 Abs. 1 der RL 95/46/EG genannten Zwecke vorgesehen werden darf und nur soweit dies in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.

Vor diesem Hintergrund stellt sich die Frage, ob die, für die Beantwortung der vom Landesgericht für Strafsachen Wien gestellten Frage, notwendigen Verkehrsdaten-aufzeichnungen beim Betreiber zulässigerweise noch vorhanden waren, obwohl die Kommunikation, auf die sich die Verkehrsdaten – nämlich Zeitpunkt und IP-Adresse – bezogen, längst beendet war. Die Daten wurden für ihren eigentlichen Zweck, der in der Herstellung und Aufrechterhaltung der Verbindung besteht, nicht mehr benötigt. Der Betreiber hat in seiner Stellungnahme behauptet, die Daten für die Kontrolle der Einhaltung seiner mit dem Teilnehmer vereinbarten Fair-Use-Policy speichern zu müssen. Dies kann als rechtmäßiger Grund für die nach § 99 Abs 1 TKG 2003 bestehende Verpflichtung zur unverzüglichen Löschung nach Beendigung der Verbindung nicht anerkannt werden. Für die Kontrolle der Einhaltung der monatlichen Daten-Volumensbeschränkungen pro Teilnehmer würde es genügen, das Volumen pro Verbindung beim Teilnehmer zu speichern und zu summieren.

Es muss daher festgestellt werden, dass der Betreiber N*** ISP GmbH gegen § 93 Abs 2 und § 99 Abs 1 TKG 2003 dadurch verstoßen hat, dass er die IP-Adresse der Betroffenen nach Abschluss der technischen und organisatorischen Abwicklung der jeweiligen Verbindung nicht gelöscht hat.

Zur Beseitigung dieses rechtswidrigen Zustandes war die vorliegende Empfehlung auf Grundlage des § 30 Abs 6 DSG 2000 auszusprechen.

11. Oktober 2006
Für die Datenschutzkommission
Der Vorsitzende:
HR des OGH Dr. SPENLING

Für die Richtigkeit
der Ausfertigung: