Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Bern, den 09. Januar 2008

EMPFEHLUNG

gemäss

Art. 29 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG),

betreffend

die Bearbeitung und Weitergabe von elektronischen Datenspuren durch die Firma X im Auftrag von Urheberrechtsinhabern

I.

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Die Firma X hat insbesondere in einer Besprechung und in einer Vorführung ihre Datenbearbeitung vorgestellt sowie in zwei Stellungnahmen den Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten (EDÖB) darüber informiert, dass sie im Auftragsverhältnis mit elektronischen Hilfsmitteln in der Schweiz Übermittlungsdaten (darunter Datum, IP-Adresse, Benutzername, etc.) von urheberrechtlich geschützten Werken aufzeichnet, welche auf peer-to-peer Netzwerken zum herunterladen (Download) angeboten werden (Aufzeichnungstätigkeit). Zudem gibt die Firma X diese aufgezeichneten Übermittlungsdaten im Anschluss an ihre Auftraggeber ins Ausland weiter.

2. Aufgrund der mit dem EDÖB abgehaltenen Sitzung und den beiden eingereichten Stellungnahmen kann die Aufzeichnungstätigkeit der Firma X wie folgt beschrieben werden:

   - Mittels der von ihr entwickelten Software (mit dem Namen „File Sharing Monitor“ in der Version 1.8.1) sucht die Firma X automatisiert in verschiedenen peer-to-peer Netzwerken anhand eines speziell berechneten elektronischen Fingerabdrucks nach angebotenen (Upload) urheberrechtlich geschützten Werken, für welche sie von dem jeweiligen Urheberrechtsinhaber (oder deren Rechtsvertreter) einen Nachforschungsauftrag erhalten hat.

   - Sobald der von der Firma X entwickelte „File Sharing Monitor“ anhand des elektronischen Fingerabdrucks ein urheberrechtlich geschütztes Werk findet, für welches die Firma X einen Nachforschungsauftrag hat, versucht dieser zu der Software des Anbieters des urheberrechtlich geschützten Werkes eine Verbindung aufzubauen, um das Werk herunterzuladen (Download).

Feldeggweg 1, 3003 Bern
Tel. 031 323 74 84, Fax 031 325 99 96
www.edoeb.admin.ch

- Kann eine Verbindung zur Software des Anbieters des urheberrechtlich geschützten Werkes aufgebaut werden, so lädt der „File Sharing Monitor“ dieses Werk automatisch ganz oder in Teilen herunter (Download) und zeichnet währenddessen einen Teil der zur Herstellung und Aufrechterhaltung der Internetverbindung zur Software des Anbieters ausgetauschten elektronischen Daten sowie weitere Daten (wie Uhrzeit und Datum) auf und speichert diese in einer Datenbank ab.

- Im Anschluss daran übermittelt die Firma X die entsprechend aufgezeichneten und abgespeicherten Daten periodisch an den jeweiligen Urheberrechtsinhaber bzw. deren Rechtsvertreter.

3. Die von den Anbietern des jeweiligen urheberrechtlich geschützten Werkes übermittelten Verbindungsdaten sind zum Austausch des Werkes notwendig und werden von der von ihm verwendeten (Standard-)Software automatisch und ohne sein zutun übermittelt, da ansonsten technisch kein Datenaustausch stattfinden kann. Der Anbieter von urheberrechtlich geschützten Werken wird von der Firma X nicht darüber informiert, dass die von ihm übermittelten Verbindungsdaten aufgezeichnet und gespeichert werden.

4. Die von der Firma X aufgezeichneten Verbindungsdaten umfassen:

   - den Benutzernamen des Nutzers des peer-to-peer Netzwerkes

   - die IP-Adresse des verwendeten Internetanschlusses

   - die GUID (spezielle Identifikationsnummer der vom Anbieter des urheberrechtlich geschützten Werkes verwendeten Software)

   - das verwendete peer-to-peer Netzwerkprotokoll (Gnutella, eDonkey oder BitTorrent)

   - den Namen und elektronischen Fingerabdruck (Hashcode) des urheberrechtlich geschützten Werkes

   - das Datum und die Uhrzeit sowie den Zeitraum der Verbindung zwischen der Software der Firma X und der Software des Anbieters des jeweiligen urheberrechtlich geschützten Werkes.

   Diese Daten werden sodann auf den Servern der Firma X in Steinhausen (ZG) gespeichert und nach Ländern und Anbietern von Internetanschlüssen sortiert. Die so erhobenen Daten werden anschliessend an die Urheberrechtsinhaber bzw. deren Rechtsvertreter ins Ausland weitergegeben und zur Identifikation des Inhabers des Internetanschlusses verwendet.

5. Zur Identifikation des Inhabers des Internetanschlusses reichen die Urheberrechtsinhaber bzw. ihre Rechtsvertreter bei den zuständigen Untersuchungsbehörden Strafklage gegen Unbekannt ein. Nachdem die zuständige Untersuchungsbehörde den Inhaber des Internetanschlusses identifiziert hat, verschaffen sich die Urheberrechtsinhaber bzw. deren Rechtsvertreter diese Identitätsdaten im Rahmen einer Akteneinsicht. Diese Daten werden dann in Abmahnverfahren verwendet, um gegenüber den betroffenen Personen Schadensersatzforderungen geltend zu machen und eine Unterlassungserklärung anzustreben. Tritt die betroffene Person nicht auf diese Forderungen ein, stellen die Inhaber der Urheberrechte bzw. deren Rechtsvertreter eine zivilrechtliche Durchsetzung ihrer Schadensersatzforderungen in Aussicht.

II.

Erwägungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten:

1. Die von der Firma X durchgeführte Datenbearbeitung zielt darauf ab, den Urheberrechtsinhabern die Möglichkeit zu eröffnen, die hinter einem Austausch urheberrechtlich geschützter Daten stehenden Personen (Inhaber des Internetanschlusses bzw. Urheberrechtsverletzer) zu bestimmen. Da dies aufgrund der Verbindungsdaten (insbesondere der IP-Adresse) im Rahmen einer Strafanzeige in der Regel möglich ist, werden namentlich IP-Adressen als personenbezogene Daten angesehen (Art. 3 lit. a DSG; Basler Kommentar zum DSG, Urs Belser zu Art. 3 DSG, Rz. 6; Artikel 29 Datenschutzgruppe, Stellungnahme 04/2007 zum Begriff „personenbezogene Daten", http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf). Da die IP-Adresse ein personenbezogenes Datum darstellt, sind alle mit ihr in Verbindung gebrachten Daten (wie in Rz. 4 aufgeführt) ebenfalls als personenbezogene Daten anzusehen. Zudem können in diesem Zusammenhang diese Daten als besonders schützenswertes Personendaten gemäss Art. 3 lit. c Ziff. 4 DSG angesehen werden, da sie im Rahmen eines Strafverfahrens zur Feststellung einer Straftat verwendet werden.

2. Unter „Bearbeiten" ist jeder Umgang mit Personendaten zu verstehen, dabei insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 Bst. e DSG). Im vorliegenden Fall beschafft, verwendet und bewahrt die Firma X personenbezogene Daten auf und gibt die so erhobenen Personendaten an die Urheberrechtsinhaber bzw. deren Rechtsvertreter ins Ausland weiter. In einem zweiten Schritt verwenden die Urheberrechtsinhaber bzw. deren Rechtsvertreter die Verbindungsdaten, um über eine Strafanzeige den Inhaber des dazugehörigen Internetanschlusses zu identifizieren. Um die von der Firma X durchgeführte Datenbearbeitung beurteilen zu können, muss diese im Gesamtkontext und nicht isoliert betrachtet werden.

3. Die urheberrechtlich geschützten Werke sowie die zum Download benötigten Verbindungsdaten (IP-Adresse), für welche die Firma X einen Nachforschungsauftrag hat, werden auf peer-to-peer Plattformen von Teilnehmern an Tauschbörsen teilweise öffentlich zugänglich gemacht. Zudem ist die Firma X ohnehin ein Tauschpartner und erhält die zur Verbindung und dem dazugehörigen Download relevanten Daten vom Anbieter der jeweiligen Datei auf freiwilliger Basis. Diese der Firma X zugänglich gemachten Verbindungsdaten fallen daher nicht unter das Fernmeldegeheimnis. Für deren Bearbeitung (insbesondere Sammlung, Verarbeitung und Weitergabe der von der Firma X gesammelten personenbezogenen Daten) ist das Datenschutzgesetz (Art. 2 Abs. 1 lit. a DSG) anwendbar.

   Im Gegensatz zu den im vorliegenden Fall ausgetauschten und damit gegenüber dem Tauschpartner zugänglich gemachten Verbindungsdaten sind die zugehörigen Identitätsdaten (wie Name, Vorname, Adresse, etc., welche lediglich dem Anbieter des Internetanschlusses bekannt sind) grundsätzlich vom Fernmeldegeheimnis geschützt. Lediglich aufgrund einer gesetzlichen Grundlage kann das Fernmeldegeheimnis durchbrochen werden. Auf diese Weise können Untersuchungsbehörden gestützt auf Art. 5 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1, BÜPF) und Art. 14 Abs. 4 BÜPF aufgrund von Verbindungsdaten die dazugehörigen Identitätsdaten von den Anbietern von Fernmeldediensten herausverlangen. Obwohl das DSG auf ein Strafverfahren keine Anwendung findet (Art. 2 Abs. 2 lit. c DSG), sind die Untersuchungsbehörden dazu berechtigt, bei der Gewährung von Akteneinsichtsrechten gegenüber den Geschädigten mögliche entgegenstehende öffentliche und private Interessen zu berücksichtigen (vgl. z.B. Art. 108 des Entwurfs der Schweizerischen Prozessordnung StPO) und

eine Interessensabwägung im Hinblick auf die Bekanntgabe der Daten durchzuführen. Zudem sind auch die Strafverfolgungsbehörden an das Amtsgeheimnis gebunden (Art. 320 StGB).

4. Die Voraussetzungen für eine Empfehlung im Sinne des DSG sind gegeben, da die Bearbeitungsmethoden grundsätzlich geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Art. 29 Abs. 1 lit. a DSG). Verstösst eine Datenbearbeitung zudem gegen die Vorschriften des Datenschutzes, kann der EDÖB gestützt auf Art. 29 Abs. 3 DSG empfehlen, die Datenbearbeitung zu ändern, einzustellen oder zu unterlassen.

5. Um die Konformität der Datenbearbeitung durch die Firma X mit dem DSG beurteilen zu können, muss diese im Hinblick auf die Voraussetzungen für eine rechtmässige Datenbearbeitung geprüft werden. Eine solche ist gegeben, wenn die Datenbearbeitung den Grundsätzen des Datenschutzes entspricht, welche namentlich sind: die Einhaltung des Rechtmässigkeitsprinzips (Art. 4 Abs. 1 DSG), des Zweckmässigkeitsprinzips (Art. 4 Abs. 3 DSG), des Transparenzprinzips (Art. 4 Abs. 2 DSG), des Verhältnismässigkeitsprinzips (Art. 4 Abs. 2 DSG) sowie die Grundsätze für eine Bekanntgabe der Daten ins Ausland (Art. 6 DSG). Falls diese nicht eingehalten werden und bei der Datenbearbeitung von einer Persönlichkeitsverletzung ausgegangen werden muss (Art. 12 DSG), ist darüber hinaus zu prüfen, ob Rechtfertigungsgründe (Art. 13 DSG) vorliegen, welche eine Datenbearbeitung dennoch ermöglichen. In diesem Rahmen kann die Firma X nach Art. 14 Abs. 2 DSG dieselben Rechtfertigungsgründe geltend machen, wie die Urheberrechtsinhaber.

Rechtmässigkeitsprinzip

6. Bis heute existiert in der Schweiz weder eine spezifische gesetzliche Grundlage, welche die systematische Erhebung von IP-Adressen in peer-to-peer Netzwerken erlaubt, noch ist eine solche Datenerhebung explizit verboten (vgl. StGB, BÜPF). Daher gelangt im vorliegenden Fall das DSG zur Anwendung. Im europäischen Ausland werden derzeit verschiedene gesetzliche Regelungen zur Bekämpfung der Film- und Musikpiraterie diskutiert.

   Da die Datenbearbeitung ohne Wissen der betroffenen Personen automatisiert und proaktiv durchgeführt wird sowie der Inhaber der Datensammlung darüber hinaus in die Lage versetzt wird, mit den gesammelten Daten im Nachgang Strafuntersuchungen gegen eine von vorne herein unbestimmte Anzahl von Personen anzustossen, vertritt der EDÖB die Meinung, dass eine solche Untersuchung explizit gesetzlich geregelt werden muss. Dies gilt vor allem, da eine solche Datenbearbeitung eine grosse Reichweite hat und die Persönlichkeitsrechte einer Vielzahl betroffener Personen tangiert werden. Der gesetzliche Rahmen sollte darüber hinaus die Beweiskraft solcher über das Internet gesammelten Daten und ihre Zulässigkeit als Beweismittel regeln.

Zweckmässigkeitsprinzip

7. Gemäss dem Zweckmässigkeitsprinzip dürfen personenbezogene Daten nur zu dem Zweck verwendet werden – eine entsprechende gesetzliche Regelung vorbehalten – der bei deren Erhebung angegeben wurde oder aus den Umständen erkennbar ist.

8. Bei der Nutzung von peer-to-peer Netzwerken besteht der Zweck der Bekanntgabe und des Austausches von IP-Adressen im Austausch von Dateien zwischen den einzelnen Nutzern des peer-to-peer Netzwerkes. Die Verwendung dieser Daten durch die Firma X zum Zwecke der Feststellung von Urheberrechtsverletzungen stellt eine Entfremdung des ursprünglich angestrebten Zwecks dar. Aus den konkreten Umständen der Nutzung eines peer-to-peer Netzwerkes ist zudem auch nicht erkennbar, dass ein Tauschpartner systematisch Daten sammelt. Daher müsste

nach datenschutzrechtlichen Gesichtspunkten die Firma X gegenüber den betroffenen Nutzern des peer-to-peer Netzwerkes den Zweck der von ihr durchgeführten Datenbearbeitung bekannt machen. Da die Firma X allerdings ihre Daten ohne Information und Wissen der betroffenen Personen erhebt, wird das Zweckmässigkeitsprinzip verletzt. In wieweit die Verletzung des Zweckmässigkeitsprinzips durch ein überwiegendes privates Interesse gerechtfertigt werden kann, wird nachfolgend geprüft (siehe Abschnitt: „Notwendigkeit eines Rechtfertigungsgrundes“).

Treu und Glauben sowie Transparenzprinzip

9. Datenbearbeitungen haben nach Treu und Glauben zu erfolgen (vgl. Art. 4 Abs. 2 DSG). Gegen den Grundsatz von Treu und Glauben verstösst z.B. derjenige, welcher heimlich Daten beschafft, ohne dabei gegen eine Rechtsnorm zu verstossen (BBl 1988 II 449). Aus diesem Prinzip ist die Anforderung abzuleiten, dass eine Datenbeschaffung für die betroffene Person transparent erfolgen muss. Dies bedeutet, dass eine Datenbeschaffung und jede weitere Datenbearbeitung grundsätzlich für die betroffene Person erkennbar sein muss, der Betroffene also aus den Umständen heraus damit rechnen muss oder er entsprechend informiert bzw. aufgeklärt wird. Je einschneidender die Datenbearbeitung in Bezug auf die Persönlichkeitsrechte ist, desto höhere Anforderungen werden an die Transparenz gestellt (vgl. U. Maurer in Basler Kommentar, Datenschutzgesetz, Maurer/Vogt. Hrsg., 2006, Art. 4 Rz. 8). Nach den Regelungen des revidierten Datenschutzgesetzes (Art. 7a rev. DSG) wird sogar eine aktive Informationspflicht gefordert, wenn es sich um besonders schützenswerte Personendaten handelt und kein überwiegendes öffentliches oder privates Interesse dem entgegensteht (BBl 2003 I 2131).

10. Die von der Firma X durchgeführte Datensammlung erfolgt ohne jedes Wissen der betroffenen Personen (sei es der Inhaber des Internetanschlusses oder der eigentliche Urheberrechtsverletzer) und muss daher als heimliche Datenbeschaffung angesehen werden. Weder auf den Webseiten der Tauschbörsen, auf welchen man die File-Sharing-Software zur Teilnahme an einem peer-to-peer Netzwerk herunterladen kann, noch über die Kommunikationskanäle, über welche File-Sharing-Programme in der Regel verfügen, wird auf die Möglichkeit hingewiesen, dass die Verbindungsdaten aufgezeichnet werden könnten. Der Inhaber des Internetanschlusses erhält von der Datenaufzeichnung in keinem Fall Kenntnis, da er im Kommunikationsprozess zwischen dem Urheberrechtsverletzer und der Firma X nicht eingebunden ist. Zudem hat die Firma X denn auch eigens zur Sammlung von solchen Verbindungsdaten eine Software (File Sharing Monitor) entwickelt, welche dazu dient systematisch und ohne Kenntnis der Betroffenen Verbindungsdaten aufzuzeichnen. Alleine schon die Konzeption der Software, welche es erlaubt unerkannt Dateien herunterzuladen ohne dabei gleichzeitig andere Dateien zum Upload bereitzustellen ist darauf angelegt, heimlich Verbindungsdaten aufzuzeichnen. Heute gestatten übliche File-Sharing Programme eine Teilnahme an einem peer-to-peer Netzwerk nur dann einen Download, wenn gleichzeitig Dateien zum Upload zur Verfügung gestellt werden. Die Software der Firma X umgeht im peer-to-peer Netzwerk einen Upload, um am Tauschgeschehen teilzunehmen. Damit täuscht die von der Firma X verwendete Software vor, sie sei ein gewöhnlicher Teilnehmer eines peer-to-peer Netzwerkes, um so inkognito bzw. ohne Wissen der betroffenen Personen (Inhaber des Internetanschlusses und/oder Urheberrechtsverletzer) Daten zu sammeln.

11. In wieweit die Verletzung des Transparenzprinzips durch ein überwiegendes privates Interesse gerechtfertigt werden kann, wird nachfolgend geprüft (siehe Abschnitt: „Notwendigkeit eines Rechtfertigungsgrundes“).

12. Weiterhin werden die von der Firma X gesammelten Daten vorwiegend mit dem Ziel gesammelt, um den Inhaber des jeweiligen Internetanschlusses zu identifizieren und anschliessend gegen-

über diesem Zivilansprüche geltend zu machen. Da die Identifizierung der Inhaber eines Internetanschlusses ausschliesslich im Rahmen einer Strafanzeige möglich ist, da die Identitätsdaten grundsätzlich durch das Fernmeldegeheimnis geschützt sind, umgehen die Urheberrechtsinhaber mit der Einleitung eines Strafverfahrens als Mittel zum Zweck zur Feststellung der Identität des Inhabers des Internetanschlusses und zur Geltendmachung von Zivilansprüchen gegenüber diesen das Fernmeldegeheimnis. Ein solches Vorgehen ist als dem Prinzip von Treu und Glauben entgegengesetzt bzw. als rechtsmissbräuchlich anzusehen, da die Urheberrechtsinhaber das Rechtsinstitut der Akteneinsicht in einem Strafverfahren gegenüber einem Urheberrechtsverletzer dazu verwenden, sich für ein Zivilverfahren gegen einen gutgläubigen Inhaber eines Internetanschlusses durch die Umgehung des Telefongeheimnisses eine bessere Ausgangslage zu verschaffen. Es liegt in diesem Falle ein Institutionenmissbrauch vor (Heinrich Honsell, Basler Kommentar zum Zivilgesetzbuch, 2. Auflage, Helbing & Lichtenhahn Verlag, Basel, 2002, Art. 2, Rz. 51). Dies gilt umso mehr, als die Urheberrechtsinhaber bzw. ihre Rechtsvertreter meist nicht einmal das Ende der Strafuntersuchung abwarten, um ihre Zivilansprüche gegen den eigentlichen Urheberrechtsverletzer geltend zu machen. Vielmehr nehmen sie bereits während der laufenden Strafuntersuchung Akteneinsicht, um die Identität der gutgläubige Inhaber des Internetanschlusses zur Geltendmachung von zivilrechtlichen Forderungen festzustellen, obwohl diese keine Urheberrechtsverletzung begangen haben müssen.

13. Daher muss im Rahmen einer rein zivilrechtlichen Geltendmachung von Schadensersatzansprüchen im vorliegenden Fall ein überwiegendes privates Interesse der Urheberrechtsinhaber abgelehnt werden. Da ein solches Vorgehen darüber hinaus gegen den Grundsatz von Treu und Glauben verstösst, erübrigt sich eine Verhältnismässigkeitsprüfung für die Datenerhebung im Hinblick auf die Anstrengung eines Zivilverfahrens. Wenn eine Durchbrechung des Fernmeldegeheimnisses im Rahmen eines Zivilverfahrens ermöglicht werden soll, bedarf es nach Meinung des EDÖB hierzu einer gesetzlichen Grundlage, welche analog wie die BÜPF im Strafverfahren die Bedingungen für eine Durchbrechung des Fernmeldegeheimnisses regelt.

Verhältnismässigkeit der Datenbearbeitung zur Anstrengung eines Strafverfahrens

14. Nachfolgend wird die Verhältnismässigkeit ausschliesslich für die von der Firma X durchgeführte Datenbearbeitung im Rahmen der Anstrengung eines Strafverfahrens geprüft.

15. Damit eine Massnahme, welche in den Persönlichkeitsbereich einer privaten Person eingreift, als verhältnismässig eingestuft werden kann, muss diese im Hinblick auf den zu erreichenden Zweck geeignet und notwendig sein. Ausserdem muss der angestrebte Zweck in einem vernünftigen Verhältnis zum Eingriff in den Persönlichkeitsbereich der privaten Person stehen (Zumutbarkeit).

Geeignetheit

16. Um eine Urheberrechtsverletzung gemäss Art. 67 URG strafrechtlich ahnden zu können, ist es notwendig, den Verletzer des Urheberrechts festzustellen. Mit den von der Firma X unternommenen Massnahmen kann aufgrund der IP-Adresse inklusive Datum und Uhrzeit ihrer Verwendung der Inhaber des jeweiligen Internetanschlusses durch Untersuchungsbehörden mittels gesetzlich legitimierter Durchbrechung des Fernmeldegeheimnisses identifiziert werden (Art. 14 Abs. 4 BÜPF, vgl. auch hierzu Kritik von Bondallaz, a.a.O. Rz. 1803ff., 1834). Diese Massnahme ist geeignet, um den Täterkreis auf diejenigen Personen einzuschränken, welche den Internetanschluss benutzen und basierend hierauf weitere Massnahmen (wie z.B. Einvernahmen, Hausdurchsuchungen und/oder Beschlagnahmungen) zu ergreifen, um den tatsächlichen Urheberrechtsverlet-

zer feststellen zu können. Daher ist die von der Firma X durchgeführte Datenbearbeitung geeignet, um eine Strafuntersuchung einzuleiten.

Erforderlichkeit

17. Die von der Firma X im Auftrag der Urheberrechtsinhaber ergriffenen Massnahmen zielen letztlich auf die Identifikation des Inhabers des Internetanschlusses ab. Für eine Anzeige bei den zuständigen Strafverfolgungsbehörden ist grundsätzlich ein erster Anhaltspunkt nötig, damit ein Strafverfahren gegen eine bestimmte Person eingeleiten werden kann. Daher kann es erforderlich sein, in diesem Rahmen eine Urheberrechtsverletzung festzustellen, da somit die Erfolgswahrscheinlichkeit der Überführung des Täters erheblich gesteigert wird.

Zumutbarkeit

18. Zur Feststellung einer Straftat, vertritt der EDÖB die Meinung, dass es einem Inhaber eines Internetanschlusses, über welchen eine Straftat begangen wurde, zuzumuten ist, einer Strafuntersuchung ausgesetzt zu werden, solange ihm hierdurch – bei Unschuldigkeit – keine ernsthaften Nachteile erwachsen. Solche können dem (unschuldigen) Inhaber eines Internetanschlusses bzw. weiteren Nutzer eines Internetanschlusses allerdings drohen, wenn dessen Identität im Rahmen des Akteneinsichtsrechts zu einem Zeitpunkt, in dem der Urheberrechtsverletzer noch nicht ermittelt wurde, den geschädigten Urheberrechtsinhabern bekannt gegeben wird. Der Tatsache, dass die Identitätsdaten hinter einer IP-Adresse grundsätzlich vom Fernmeldegeheimnis geschützt sind, ist im Rahmen des Auskunftsrechts der Geschädigten nach Meinung des EDÖB zwingend Rechnung zu tragen. Für die Urheberrechtsinhaber als Geschädigte ist es für die Wahrnehmung ihrer Mitwirkungs- und Kontrollrechte (vgl. Hauser/Schweri a.a.O, § 38 Rz. 5) nicht notwendig, die Identität des Inhabers des Internetanschlusses zu erhalten, welcher keine Urheberrechtsverletzung begangen hat. Ausserdem können Sie ihre zivilrechtlichen Ansprüchen gegenüber dem Urheberrechtsverletzer im Strafverfahren adhäsionsweise geltend machen. Hingegen ist dem überführten Urheberrechtsverletzer die Bekanntgabe seiner Identität gegenüber den geschädigten Urheberrechtsinhabern sehr wohl zuzumuten.

Notwendigkeit eines Rechtfertigungsgrundes

19. Die Aufzeichnung der Verbindungsdaten durch den „File Sharing Monitor“ stellt aufgrund der oben genannten Gründe (Rz. 6-19) eine Persönlichkeitsverletzung gemäss Art. 12 Abs. 2 DSG dar, welche zur Anstrengung eines Strafverfahrens eines Rechtfertigungsgrundes nach Art. 13 Abs. 1 DSG bedarf. Art. 13 Abs. 1 DSG sieht als mögliche Rechtfertigungsgründe die Einwilligung des Verletzten, ein überwiegendes öffentliches oder privates Interesse oder das Gesetz vor. Bei der Datenbearbeitung der Personendaten durch die Firma X liegt keine Einwilligung der betroffenen Personen (weder des Inhabers der IP-Adresse noch des Urheberrechtsverletzers) vor, da die Datenerhebung ohne deren Wissen erfolgt. Während vom gutgläubigen Inhaber eines Internetanschlusses nie von einer Einwilligung ausgegangen werden kann, ist für den Urheberrechtsverletzer zu prüfen, ob er mit einer solchen Datenerhebung rechnen musste. Im vorliegenden Fall kann nicht von einer impliziten Einwilligung des Urheberrechtsverletzers ausgegangen werden, da die Daten lediglich zum Zwecke eines Datentransfers (urheberrechtlich geschütztes Werk in elektronischer Form) zwischen zwei Computerprogrammen ausgetauscht und übertragen werden und der gewöhnliche Nutzer nicht davon ausgehen kann, dass der Tauschpartner von diesen Übertragungsdaten ohne weiteres Zutun Kenntnis erhält. So hat auch die Firma X eigens eine spezielle Software („File Sharing Monitor“) entwickelt, um diese Daten überhaupt systematisch auszulesen und speichern zu können. Weiterhin ist ebenfalls keine gesetzliche Grundlage oder ein überwie-

gendes öffentliches Interesse für die von der Firma X durchgeführte Datenbearbeitung ersichtlich. Dennoch kann sich der Urheberrechtsverletzer im Gegensatz zum gutgläubigen Inhaber eines Internetanschlusses aufgrund der von ihm begangenen Straftat nicht auf seine Gutgläubigkeit berufen.

20. Damit ein überwiegendes privates Interesse angenommen werden kann, müssen gewisse Anforderungen erfüllt sein. Art. 13 Abs. 2 DSG enthält eine Aufzählung von sechs nicht abschliessenden Rechtfertigungsgründe, welche dem Richter einen gewissen Anhaltspunkt für die Interessenabwägung an die Hand geben sollen. So ist etwa „ein Beschaffen von Daten mit unrechtmässigen Mitteln nur selten, ein Beschaffen wider Treu und Glauben praktisch überhaupt nie zu rechtfertigen“, während sich für eine blosse unrichtige Datenbearbeitung wohl eher ein Rechtfertigungsgrund finden lässt. Hierbei lassen sich die Rechtfertigungsgründe grundsätzlich in vier Gruppen einteilen ([direkte] wirtschaftliche Tätigkeiten, insbesondere Vertragsabschluss, wirtschaftlicher Wettbewerb, Kreditüberprüfung; Veröffentlichung in einem Medium; nicht personenbezogene Datenbearbeitung sowie Daten einer Person des öffentlichen Lebens bezüglich ihres Wirkens in der Öffentlichkeit). Ob ein Rechtfertigungsgrund gegeben ist, muss aufgrund der konkreten Umstände im Einzelfall anhand einer sorgfältigen Interessensabwägung entscheiden werden (Urteil der EDSK vom 21. November 1996, VPB 62.42B, E. V 1b). Als schützenswerte Interessen können hierbei alle „Interessen von allgemein anerkanntem Wert“ angesehen werden (A. Bucher, natürliche Personen, S. 536 in Basler Kommentar zum DSG Corrado Rampini zu Art. 13 DSG Rz. 22).

21. Eine von der Firma X vorgenommene Datenbearbeitung und die anschliessende Einleitung eines Strafverfahrens (durch die Urheberrechtsinhaber bzw. deren Rechtsvertreter) zur Erlangung der sich hinter einer IP-Adresse verbergenden Identitätsdaten für die Anstrengung eines Zivilverfahrens verstossen gegen das Prinzip von Treu und Glauben. Eine solche Datenbearbeitung zur Geltendmachung von Zivilansprüchen kann daher nicht gerechtfertigt werden (vgl. Rz. 12).

22. Aus Art. 13 Abs. 2 DSG kann im vorliegenden Fall nur für Einleitung eines Strafverfahrens ein überwiegendes privates Interesse als Rechtfertigungsgrund entnommen werden, wobei allerdings eine Interessensabwägung entwickelt werden muss (vgl. Rz. 14ff.).

23. Bei der Verfolgung von strafrechtlich relevanten Verstössen gegen das Urheberrecht haben die Inhaber des Urheberrechts ein Interesse an der strafrechtlichen Ahndung solcher Verletzungen und im Nachgang an das Strafverfahren als Geschädigter ein Interesse an Entschädigungszahlungen, um den so entstandenen wirtschaftlichen Schaden (lucrum cessans) zu kompensieren. Diesen Interessen stehen die Persönlichkeitsrechte, insbesondere die informationelle Selbstbestimmung, der betroffenen Personen (Inhaber des Internetanschlusses und Urheberrechtsverletzer) gegenüber.

24. Eine Urheberrechtsverletzung gemäss Art. 67 URG ist nach Schweizer Recht ein Antragsdelikt. Damit eine Untersuchungsbehörde überhaupt ein Untersuchungsverfahren eröffnet, ist es notwendig, einen Anfangsverdacht einer Verletzung eines Urheberrechts festzustellen. Daher müssen gewisse Anhaltspunkte vorliegen, welche eine mutmassliche Urheberrechtsverletzung gemäss Art. 67 URG begründen. Sogar für eine heimliche Datenbearbeitung kann in diesem Rahmen ein ausreichender Rechtfertigungsgrund gegeben sein, wenn die Gefahr besteht, dass eine vorherige Anzeige aufgrund des Transparenzprinzips ein Strafverfahren verunmöglicht oder wesentlich erschwert, da der Urheberrechtsverletzer wichtige Beweismittel vernichten könnte bzw. diese gar nicht erst erhoben werden könnten.

25. Nach erfolgter Anzeige gegen Unbekannt ist es Sache der jeweiligen Strafverfolgungsbehörden, den tatsächlichen Sachverhalt zu ermitteln und den Täter ausfindig zu machen. Grundsätzlich stehen den Geschädigten im Rahmen eines Strafverfahrens Parteirechte, insbesondere Mitwirkungs- und Kontrollrechte zu (Hauser, Schweri, Schweizerisches Strafprozessrecht, 4. neu überarbeitete und ergänzte Auflage, Helbing & Lichtenhahn, Basel, Genf, München, 1999, §38, Rz. 5, 7). Hierbei beurteilt sich die Frage der Akteneinsicht nach den allgemeinen Verfahrensgrundsätzen wie sie auch in dem Entwurf zur Schweizerischen Strafprozessordnung (StPO, http://www.admin.ch/ch/d/ff/2007/6977.pdf) geregelt sind. Gemäss Art. 108 StPO darf die Einsichtnahme verweigert oder beschränkt werden, wenn ihr wesentliche öffentliche und private Interessen entgegenstehen oder wenn ein begründeter Verdacht besteht, dass eine Partei ihre Rechte missbraucht (BBl 2007 Nr. 42 S. 6977). In BGE 95 I 109 stellt das Bundesgericht fest, dass das Akteneinsichtsrecht (sowohl in abgeschlossenen als auch in laufenden Verfahren) seine Grenzen an den öffentlichen Interessen des Staates oder den berechtigten Geheimhaltungsinteressen Privater findet. Aus diesem Grund kann es geboten sein, im Rahmen von laufenden Untersuchungen das Akteneinsichtsrecht zu verweigern. Im vorliegenden Fall wird das Akteneinsichtsrecht dazu gebraucht, gegenüber dem Inhaber eines Internetanschlusses ein Zivilverfahren zu einem Zeitpunkt anzustrengen, in welchem das Strafverfahren noch nicht abgeschlossen ist und der Urheberrechtsverletzer noch nicht feststeht. Zudem hat die geschädigte Partei ausschliesslich über das Akteneinsichtsrecht die Möglichkeit die sich hinter einer IP-Adresse verbergende Identität des Anschlussinhabers zu erlangen. In einem rein zivilrechtlichen Verfahren besteht eine solche Möglichkeit nicht, da die Identität hinter einer IP-Adresse vom Fernmeldegeheimnis geschützt ist. Wird die Identität des Inhabers eines Internetanschlusses dem Urheberrechtsinhaber bekannt, kann sich der Inhaber des Internetanschlusses mit Zivilforderungen konfrontiert sehen, obwohl er möglicherweise keine Urheberrechtsverletzung begangen hat. Der EDÖB vertritt die Meinung, dass eine solche Durchbrechung des Fernmeldegeheimnisses nur aufgrund einer gesetzlichen Grundlage möglich sein darf. Auf der anderen Seite entsteht dem Urheberrechtsinhaber kein nicht wieder gutzumachender Nachteil, wenn das Akteneinsichtsrecht erst nach erfolgreichem Abschluss der Strafuntersuchung gewährt wird und der Urheberrechtsverletzer gefunden wurde. Selbst eine adhäsionsweise Geltendmachung der Zivilansprüche im Rahmen des Strafverfahrens würde ausreichen, um die Zivilforderungen des Urheberrechtsinhabers angemessen zu berücksichtigen. Daher gebietet es das schützenswerte private Interesse des Anschlussinhabers, dass seine Identität nur dann bekannt gegeben wird, wenn ihm eine Urheberrechtsverletzung nachgewiesen werden konnte und er sich daher nicht auf seine Gutgläubigkeit berufen kann.

26. Dies gilt umso mehr als gemäss Art. 8 Abs. 1 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (SR 0.101, EMRK) jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz hat. Dieses Recht kann gemäss Art. 8 Abs. 2 EMRK von einer Behörde aufgrund einer gesetzlichen Grundlage (z.B. durch die BÜPF in Strafverfahren) eingeschränkt werden. Da sich allerdings Art. 8 Abs. 1 EMRK nicht nur an den Gesetzgeber, sondern auch an die anwendenden Behörden (hier die Strafverfolgungsbehörden) richtet (Stéphane Bondallaz, La protection des personnes et de leur données dans les télécommunications, Schulthess, Zürich, Basel, Genf, 2007, Rz. 334, S. 103), sind auch diese angehalten, die Persönlichkeitsrechte im Rahmen des Akteneinsichtsrechts zu schützen. Daher sollte in jedem Fall verhindert werden, dass die Identität eines Inhabers des Internetzugangs (welche durch das Fernmeldegeheimnis geschützt ist und nur aufgrund einer gesetzlichen Grundlage durchbrochen werden kann) bekannt wird, solange diesem keine Schuld an der Urheberrechtsverletzung nachgewiesen werden kann.

27. In der derzeitigen Praxis kann aufgrund des von den Untersuchungsbehörden gewährten Akteneinsichtsrechts, die von der Firma X unternommene Datenbearbeitung nicht auf den Zweck der

strafrechtlichen Verfolgung der Urheberrechtsverletzung nach Art. 67 URG beschränkt werden. Vielmehr werden über den Institutionsmissbrauch des Akteneinsichtsrechts diese von der Firma X erhobenen Daten unrechtmässig zur Anstrengung von Zivilverfahren gegen die jeweiligen gutgläubigen Inhaber des Internetanschlusses verwendet. Damit wird letztendlich im zivilrechtlichen Bereich das Fernmeldegeheimnis umgangen und die Urheberrechtsinhaber machen hiervon auch regen Gebrauch. Da hierdurch die Persönlichkeitsrechte einer unbeschränkten Anzahl gutgläubiger Inhaber von Internetanschlüssen verletzt werden, kann auch im vorliegenden Fall die Anstrengung eines Strafverfahrens nicht als ausreichender Rechtfertigungsgrund angesehen werden, solange nicht gewährleistet werden kann, dass die Identität gutgläubiger Inhaber von Internetanschlüssen im Strafverfahren geschützt werden.

Notwendigkeit einer gesetzlichen Grundlage und Schlussfolgerung

28. Faktisch ist der Umweg über die Einleitung eines Strafverfahrens, um so die Identität des Inhabers des Internetanschlusses zu erhalten, eine Umgehung des Fernmeldegeheimnisses im privatrechtlichen Bereich. Gemäss Art. 35 Abs. 1 BV ist der Gesetzgeber dazu angehalten, die Grundrechte, welche die Privatsphäre schützen auch im privatrechtlichen Bereich durchzusetzen (S. Bondallaz, a.a.O., Rz. 265). Eine Durchbrechung des Fernmeldegeheimnisses bedarf daher (wenn eine solche vom Gesetzgeber gewünscht wird) aus Sicht des EDÖB einer expliziten gesetzlichen Grundlage, welche regelt, wann, wie und unter welchen Bedingungen eine solche Durchbrechung möglich sein sollte. Das blosse Ausnutzen einer Gesetzeslücke kann hierfür nicht ausreichen.

29. Bereits in der parlamentarischen Diskussion zu Art. 51 URG im Hinblick auf die Durchsetzung der Auskunftspflicht von Nutzern urheberrechtlicher Werke gegenüber den Verwertungsgesellschaften präzisiert der Gesetzgeber in der Botschaft hierzu, dass die Erteilung von Auskünften zur Geltendmachung zivilrechtlicher Ansprüche nicht hoheitlich durchgesetzt werden kann, sondern er verweist ausdrücklich auf den privatrechtlichen Klageweg (BBl 1989 III 561). Auch in der kürzlich geführten parlamentarischen Diskussion zur Umsetzung des WIPO-Abkommens wurde ein Ausbau der verwandten Schutzrechte diskutiert. Dieser wurde allerdings vom Gesetzgeber abgelehnt, da kein ersichtlicher Grund besteht von der 1992 vorgenommenen Interessensabwägung abzuweichen (BBl 2006 3404). Somit hat der Gesetzgeber bisher für eine Durchsetzung von zivilrechtlichen Urheberrechtsansprüchen mit hoheitlichen Mitteln noch keine gesetzliche Grundlage geschaffen.

30. Aus datenschutzrechtlicher Sicht könnte daher einzig die Sammlung von IP-Adressen inklusive Zeitstempel zum Zwecke der Strafverfolgung als ein überwiegendes privates Interesse angesehen werden (vgl. Rz. 19-24). Solange allerdings (sowohl in der Schweiz wie auch im Ausland) nicht gewährleistet ist, dass die Identität der Inhaber eines Internetanschlusses solange geschützt bleibt, bis diese der Urheberrechtsverletzung überführt werden konnten, ist die Datenbearbeitung durch die Firma X und die Urheberrechtsinhaber bzw. deren Rechtsvertreter in ihrer Gesamtheit dazu geeignet, die Persönlichkeit betroffener Personen (Inhaber von Internetanschlüssen, welche keine Urheberrechtsverletzung begangen haben) zu verletzen (vgl. Rz. 25-27).

31. Da nicht ausgeschlossen werden kann, dass die von der Firma X erhobenen Daten in der oben beschriebenen Form zur Identifikation eines Inhabers eines Internetanschlusses, welcher keine Urheberrechtsverletzung begangen hat, verwendet werden, ist die durchgeführte Datenbearbeitung insgesamt als unrechtmässig zu qualifizieren.

32. Zu prüfen ist auch, ob und in wie weit weniger schwerwiegende Möglichkeiten bestehen, um Urheberrechtsverletzungen zu bekämpfen. Hierbei ist vor allem an Massnahmen wie spezielle Filter

zu denken, die von Anbietern von Internetzugängen genutzt werden können, um den Austausch spezifischer Dateien in P2P-Netzwerken auf der Basis einer Datenbank urheberrechtlich geschützter Werke zu unterbinden. Solche Technologien existieren bereits heute[1].

[1] Vgl. http://www.juriscom.net/etc

III.

Aufgrund dieser Erwägungen empfiehlt
der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte:

Die Firma X stellt die von ihr praktizierte Datenbearbeitung unverzüglich ein, solange keine ausreichende gesetzliche Grundlage für eine zivilrechtliche Nutzung der durch sie erhobenen Daten besteht.

Die Firma X teilt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) innerhalb von 30 Tagen ab Erhalt dieser Empfehlung mit, ob sie die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung nicht befolgt oder abgelehnt, so kann der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen (Art. 29 Abs. 4 DSG).

Bei Annahme der Empfehlung gilt der Fristablauf (30 Tage) gleichzeitig als Fristbeginn für die Umsetzung der genannten Massnahme.

Die vorliegende Empfehlung wird in Anwendung von Art. 30 Abs. 2 DSG in anonymisierter Form publiziert.

EIDGENÖSSISCHER DATENSCHUTZ- UND
ÖFFENTLICHKEITSBEAUFTRAGTER

Hanspeter Thür