BVGer A-3144/2008 vom 27. Mai 2009

Bundesverwaltungsgericht, 2009-05-27, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/bvger_A-3144_2008

FR: TAF A-3144/2008 du 27 mai 2009

IT: TAF A-3144/2008 del 27 maggio 2009

Regeste

Datenschutz

Erwägungen

E. 1

Der EDÖB klärt von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler, Art. 29 Abs. 1 Bst. a DSG). Aufgrund seiner Abklärungen kann er empfehlen, das Bearbeiten zu ändern oder zu unterlassen (Art. 29 Abs. 3 DSG). Wird eine solche Empfehlung nicht befolgt oder abgelehnt, kann er die Angelegenheit dem Bundesverwaltungsgericht auf dem Klageweg zum Entscheid vorlegen (Art. 29 Abs. 4 DSG i.V.m. Art. 35 Bst. b des Verwaltungsgerichtsgesetzes vom 17. Juni 2005 [VGG, SR 173.32]). Die vorliegende, auf das DSG gestützte Klage richtet sich gegen die Nichtbefolgung bzw. die Ablehnung einer Empfehlung des EDÖB durch die Beklagte. Diese bestreitet die Anwendbarkeit des DSG und hält den EDÖB aus verschiedenen Gründen für sachlich und örtlich unzuständig. Zunächst ist daher abzuklären, ob das DSG im vorliegenden Verfahren überhaupt Anwendung findet und der Kläger zur Abgabe der fraglichen Empfehlung zuständig sowie zu deren Weiterzug an das Bundesverwaltungsgericht legitimiert war.

E. 2.1

Das DSG gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen und Bundesorgane (Art. 2 Abs. 1 DSG).

E. 2.2.1

Unter Personendaten (Daten) fallen nach Art. 3 Bst. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Darunter ist jede Art von Information zu verstehen, die auf die Vermittlung oder die Aufbewahrung von Kenntnissen ausgerichtet ist, ungeachtet, ob es sich dabei um eine Tatsachenfeststellung oder um ein Werturteil handelt. Unerheblich ist auch, ob eine Aussage als Zeichen, Wort, Bild, Ton oder Kombinationen aus diesen auftritt und auf welcher Art von Datenträger die Informationen gespeichert sind. Entscheidend ist, dass sich die Angaben einer oder mehreren Personen zuordnen lassen (Urs Belser, in: Maurer-Lambrou/Vogt [Hrsg.], Datenschutzgesetz, Basler Kommentar, 2. Aufl., Basel 2006, Rz. 5 zu Art. 3 DSG). Eine Person ist dann bestimmt, wenn sich aus der Information selbst ergibt, dass es sich genau um diese Person handelt. Bestimmbar ist sie dann, wenn aus dem Kontext einer Information auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt aber nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand für die Bestimmung der betroffenen Personen derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent

diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor (vgl. Botschaft des Bundesrates vom 23. März 1988 zum DSG, Bundesblatt [BBl] 1988 II, S. 444 f.). Ob eine Person bestimmbar ist, muss anhand objektiver Kriterien im konkreten Fall beurteilt werden, wobei insbesondere auch die Möglichkeiten der Technik, wie zum Beispiel die beim Internet verfügbaren Suchwerkzeuge, mitzuberücksichtigen sind. Entscheidend ist nicht, ob derjenige, der die Daten bearbeitet, den für eine Identifizierung erforderlichen Aufwand betreiben kann oder will, sondern ob damit gerechnet werden muss, dass ein Dritter, der ein Interesse an diesen Angaben hat, bereit ist, eine Identifizierung vorzunehmen (Belser, a.a.O., Rz. 6 zu Art. 3 DSG; David Rosenthal, in: Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Rz. 24 f. zu Art. 3 DSG).

E. 2.2.2

Das Internet ist ein Netzwerk von Rechnernetzwerken, durch das weltweit Daten ausgetauscht werden. Grundsätzlich kann jeder Computer mit jedem anderen verbunden werden und in Kommunikation treten. Dabei findet der Datenaustausch über technisch normierte Internetprotokolle statt. Damit jeder an das Internet angeschlossene Rechner identifiziert werden kann und externe Daten empfangen werden können, wird dem Rechner eine spezifische Adresse, die so genannte "Internetworking Protocol Address" (IP-Adresse), zugeordnet (vgl. Urteil des Bundesgerichts 4C.9/2002 vom 23. Juli 2002 E. 4). Dabei handelt es sich um einen numerischen Kommunikationsparameter, der die Identifikation einer insbesondere aus Netzrechnern oder -servern bestehenden Internet-Domain sowie der Benutzerrechner, die an den Verbindungen in diesem Netz beteiligt sind, ermöglicht (vgl. Anhang der Verordnung vom 6. Oktober 1997 über die Adressierungselemente im Fernmeldebereich [AEFV, SR 784.104]). Die IP-Adresse ist Dreh- und Angelpunkt beim Datenaustausch; über sie können bei den Internet-Zugangsanbietern Name und weitere persönliche Daten der Internetnutzer ermittelt werden (CHRISTIAN SCHWARZENEGGER, Urheberstrafrecht und Filesharing in P2P-Netzwerken - Die Strafbarkeit der Anbieter, Downloader, Verbreiter von Filesharing-Software und Hash-Link-Setzer, in: Internet-Recht und Strafrecht, 4. Tagungsband 2004, Bern 2005, S. 248). Wird einem Rechner eine IP-Adresse fest zugewiesen, spricht man von einer statischen IP-Adresse. Wählt sich ein Benutzer über einen Internet-Dienstanbieter ins Internet ein, erhält er meist eine dynamische IP-Adresse, das heisst seinem Computer wird bei jeder Verbindungsaufnahme neu irgendeine freie Adresse aus dem vorhandenen Pool des Providers zugewiesen.

E. 2.2.3

Hinsichtlich der Qualifikation von IP-Adressen als Personendaten rechtfertigt sich eine vergleichende Betrachtung der Rechtslage in der Europäischen Union: Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (nachfolgend Datenschutzgruppe) wurde durch Art. 29 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 eingesetzt und ist ein unabhängiges EU-Beratungsgremium für Datenschutzfragen. In ihrer am 20. Juni 2007 angenommenen Stellungnahme 4/2007 zum Begriff "personenbezogene Daten" stuft die Datenschutzgruppe mit Verweis auf ein früheres Arbeitspapier (Arbeitsdokument WP 37, Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz, angenommen am 21. November 2000, insbesondere S. 17) IP-Adressen als Daten ein, die sich auf eine bestimmbare Person beziehen. Internet-Zugangsanbieter und Verwalter von lokalen Netzwerken könnten ohne grossen Aufwand Internetnutzer identifizieren, denen sie

IP-Adressen zugewiesen hätten, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internetnutzer zugeteilte dynamische IP-Adresse einfügen würden. Dasselbe lasse sich von den Internet-Dienstanbietern sagen, die in ihren HTTP-Servern Protokolle führen würden. In diesen Fällen bestehe kein Zweifel, dass man von personenbezogenen Daten im Sinne von Art. 2 Bst. a der Richtlinie 95/46/EG reden könne. Weiter wird in der Stellungnahme zum Begriff "personenbezogene Daten" ausdrücklich auf jene Fälle hingewiesen, in denen der Zweck der Verarbeitung von IP-Adressen in der Identifizierung der Computernutzer besteht, beispielsweise durch Inhaber von Urheberrechten zur strafrechtlichen Verfolgung wegen Verletzung von Rechten an geistigem Eigentum. Vor allem in diesen Fällen gehe der für die Verarbeitung Verantwortliche vom Vorhandensein der Mittel aus, die zur Identifizierung der betreffenden Personen "vernünftigerweise eingesetzt werden könnten", zum Beispiel von den Gerichten, bei denen Beschwerde eingelegt worden sei. Andernfalls sei die Erhebung der Informationen nicht sinnvoll. Einen Sonderfall würden IP-Adressen bilden, die unter bestimmten Umständen aus verschiedenen technischen und organisatorischen Gründen keine Identifizierung des Nutzers gestatten würden, wie beispielsweise bei einem Computer in einem Internet-Café, in dem keine Identifizierung der Kunden gefordert werde. Es könne argumentiert werden, dass hier keine personenbezogenen Daten vorlägen, da der Nutzer unter Einsatz vernünftiger Mittel nicht identifiziert werden könne. In diesem Fall sei jedoch zu berücksichtigen, dass ein Internet-Dienstanbieter in der Regel nicht wissen könne, ob eine bestimmte IP-Adresse die Identifizierung ermögliche oder nicht. Wenn der Internet-Dienstanbieter also nicht mit absoluter Sicherheit erkennen könne, dass die Daten zu nicht bestimmbaren Benutzern gehören würden, müsse er sicherheitshalber alle IP-Informationen wie personenbezogene Daten behandeln (Stellungnahme, S. 19 f.).

E. 2.2.4

Bei IP-Adressen handelt es sich um technische Informationen, die eine eindeutige Identifizierung eines Rechners zulassen. Dabei können statische IP-Adressen, die einem Rechner fest zugeteilt sind, wie die Beklagte in ihrer Duplik selber darlegt, vergleichbar einer Telefonnummer als Personendaten qualifiziert werden. Im Ergebnis muss dasselbe aber auch für dynamische IP-Adressen gelten: Zwar können weder die Beklagte noch die Urheberrechtsinhaber selber die hinter einer IP-Adresse stehende Person bestimmen. Der Provider muss diese Information nur im Zusammenhang mit der Verfolgung von Straftaten und nur gegenüber Behörden offenlegen. Die Person ist daher lediglich anhand der IP-Adresse nicht bestimmbar (ROSENTHAL, a.a.O., Rz. 27 zu Art. 3 DSG). Wird jedoch eine Straftat verübt, ändert sich die Situation. Nicht nur steigt das Interesse an der Bestimmung der Person hinter der IP-Adresse, mit der Einleitung einer Strafuntersuchung erhält der Urheberrechtsinhaber auch indirekt das Mittel in die Hand, die Person zu identifizieren. Dadurch werden die betreffenden Aufzeichnungen automatisch zu Personendaten auch bezüglich der so ermittelbaren bzw. ermittelten Person und nicht mehr nur des registrierten Inhabers der IP-Adresse (ROSENTHAL, a.a.O., Rz. 27 zu Art. 3 DSG). Wie die Praxis zeigt, sind gerade Urheberrechtsinhaber bereit, strafrechtlich vorzugehen, um die Identifizierung der Daten von Internetnutzern zu erwirken. Sie können, objektiv betrachtet, ein konkretes Interesse an der entsprechenden Information für sich beanspruchen. Daher ist auch damit zu rechnen, dass ein in seinen Rechten verletzter Urheberrechtsinhaber den nötigen Aufwand auf sich nimmt, diese Daten zu identifizieren. Ob sodann ein Strafverfahren zum gewünschten Erfolg führt oder allenfalls im konkreten Fall vorzeitig eingestellt wird, ändert dagegen nichts an der grundsätzlichen

Bestimmbarkeit der Daten. In diesem Sinne erachtet auch die Datenschutzgruppe der Europäischen Union dynamische IP-Adressen als personenbezogene Daten gemäss Art. 2 Bst. a der Richtlinie 95/46/EG, deren Definition von Personendaten sehr ähnlich ist mit derjenigen in Art. 3 Bst. a DSG. IP-Adressen sind folglich entgegen der Ansicht der Beklagten als Personendaten im Sinne des DSG anzusehen.

E. 2.2.5

Hingegen handelt es sich - entgegen dem Vorbringen des Klägers - bei IP-Adressen nicht um besonders schützenswerte Personendaten gemäss Art. 3 Bst. c Ziff. 4 DSG. Hierunter fallen Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen. Wie gesehen kann es zwar sein, dass eine IP-Adresse zur Identifizierung einer Person Eingang in ein Strafverfahren findet. Sie stellt deswegen aber für sich allein betrachtet keine Angabe über Verfolgungen und Verurteilungen dar. Art. 3 Bst. c Ziff. 4 DSG will aber gerade solche Daten besonders schützen, da diese die Persönlichkeitsrechte betroffener Personen stärker gefährden können.

E. 2.3.1

Bearbeiten im Sinne von Art. 2 Abs. 1 DSG bedeutet jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 Bst. e DSG).

E. 2.3.2

Im vorliegenden Fall interessiert vorab das Beschaffen, Aufbewahren und Bekanntgeben von IP-Adressen durch die Beklagte. Diese macht geltend, sie sammle nur technische Informationen und keine Personendaten.

E. 2.3.3

Die Beklagte durchsucht im Auftrag von Urheberrechtsinhabern P2P-Netzwerke auf Verletzungen derer Rechte hin. Dazu verwendet sie eine von ihr entwickelte Software (File Sharing Monitor). Dieser Monitor verhält sich im P2P-Netz wie ein gewöhnlicher P2P-Client (Rechner des Internetnutzers). Allerdings ist ein Upload - auch während des Download-Prozesses - nicht möglich. Stösst die Beklagte auf ein urheberrechtlich geschütztes Werk, lädt sie dieses herunter, wobei unter anderem folgende Daten aufgezeichnet werden: IP-Adresse des Internetanschlusses, der das Werk anbietet, P2P-Benutzername des Anbieters, das verwendete P2P-Netzwerk, Name und elektronischer Fingerprint des Werks (Hashcode) sowie Datum und Uhrzeit des Downloads. Daraufhin werden diese Daten den Urheberrechtsinhabern übermittelt. Indem die Beklagte Informationen, die als Personendaten zu qualifizieren sind, sammelt, diese speichert und schliesslich weitergibt, erfüllt sie die Voraussetzung des Bearbeitens gemäss Art. 2 Abs. 1 i.V.m. Art. 3 Bst. e DSG. Dies wird von ihr insofern auch nicht bestritten, als sie selber ausführt, Informationen zu sammeln.

E. 2.4

Es kann somit festgehalten werden, dass die Beklagte Personendaten bearbeitet. Die Anwendbarkeit des DSG hängt indessen noch von weiteren Faktoren ab, die es im Folgenden zu prüfen gilt.

E. 3

Fraglich ist, ob eine der Ausnahmen von Art. 2 Abs. 2 DSG zur Anwendung kommt, die den Geltungsbereich des DSG ausschliessen. Gemäss Art. 2 Abs. 2 Bst. c DSG ist das DSG nicht anwendbar auf hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren.

E. 3.1

Die Beklagte ist der Ansicht, mit der Einleitung von Strafverfahren und allfälligen späteren Zivilprozessen lägen Verfahren im Sinne von Art. 2 Abs. 2 Bst. c DSG vor, welche die Anwendbarkeit des DSG ausschliessen würden. Der Ausschlussgrund sei bereits auf die Sammlung der technischen Informationen im Vorfeld der Verfahrenseinleitung anwendbar, da diese Tätigkeit ausschliesslich im Hinblick auf die Einleitung der Straf- und allfälliger anschliessender Zivilverfahren erfolge. Der Kläger vertritt demgegenüber die Meinung, dass eine solche Ausdehnung des Ausschlusses des Geltungsbereichs des DSG weder aus dem Wortlaut der Bestimmung ersichtlich sei noch dem Willen des Gesetzgebers entspreche. Art. 2 Abs. 2 Bst. c DSG sei daher nicht schon im Vorfeld eines hängigen Verfahrens anwendbar.

E. 3.2

Art. 2 Abs. 2 Bst. c DSG schliesst die Anwendung des DSG auf bestimmte hängige Verfahren aus. Es stellt sich somit die Frage, wann ein Verfahren als hängig gilt. Vorliegend interessiert dabei insbesondere die Festlegung des Beginns eines Verfahrens. Dies ist jeweils von Fall zu Fall zu prüfen (vgl. Gutachten des Eidgenössischen Datenschutzbeauftragen vom 12. Juni 2001, Ziff. 4, veröffentlicht in Verwaltungspraxis der Bundesbehörden [VPB] 65.98).

E. 3.2.1

Die Beklagte stützt sich in ihrer Begründung im Wesentlichen auf die Dissertation von LORENZ DROESE (Die Akteneinsicht des Geschädigten in der Strafuntersuchung vor dem Hintergrund zivilprozessualer Informationsinteressen, Diss. Luzern, Zürich/Basel/Genf 2008, S. 262 f.). Dieser vertritt die Ansicht, die Informationssammlung für den Zivilprozess sei als dessen Bestandteil zu betrachten und vom sachlichen Geltungsbereich des DSG auszunehmen. Die Gewährung von Akteneinsicht und die Verwendung von Informationen oder Beweismitteln, die durch die Akteneinsicht erlangt worden seien, würden eine Bearbeitung von Personendaten darstellen (vgl. auch das zitierte Urteil des Bundesgerichts 1P.613/1990 vom 27. März 1991 E. 5.b, veröffentlicht in Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht [ZBl] 1991, S. 543 ff.). Unproblematisch erscheine die Konstellation, in welcher in einem hängigen Strafverfahren erlangte Informationen in einem ebenfalls bereits hängigen Zivilverfahren eingebracht würden. Diesfalls sei die Anwendung des DSG ausgeschlossen und der Persönlichkeitsschutz der Betroffenen durch das jeweilige Prozessrecht gewährleistet. Gleiches gelte für die Akteneinsicht als solche. Weniger klar erscheine demgegenüber die Situation, wo Informationen oder Beweismittel, die mittels Akteneinsicht in einem inzwischen erledigten (Straf-) Verfahren erlangt worden seien, in einem späteren Zivilprozess verwendet werden sollten. Da aber im von der Verhandlungsmaxime beherrschten Zivilprozess der Prozessstoff durch die Parteien gesammelt werden müsse, sei auch die Prozessvorbereitung zum Zivilprozess zu zählen und damit von der Anwendung des DSG auszunehmen (DROESE, a.a.O., S. 263 ff.).

E. 3.2.2

Der Grundgedanke, weshalb die in Art. 2 Abs. 2 Bst. c DSG erwähnten Verfahren vom DSG nicht erfasst werden, liegt darin, dass in hängigen Verfahren bereits spezialgesetzliche Normen die Persönlichkeit von betroffenen Personen schützen sollen. Käme nun das DSG ebenfalls zur Anwendung, würden verschiedene Gesetze denselben Bereich regeln, was zu Rechtsunsicherheit, Normenkonflikten und schliesslich zu Verfahrensverzögerungen führen würde (DAVID ROSENTHAL/YVONNE JÖHRI, in: Rosenthal/Jöhri, a.a.O., Rz. 29 zu Art. 2 DSG; Urs Maurer-Lambrou/Simon Kunz, in: Maurer-Lambrou/Vogt [Hrsg.], a.a.O., Rz. 27 zu Art. 2 DSG; Botschaft zum DSG, BBl 1988 II, S. 443).

E. 3.2.3

Die Beklagte sammelt und speichert Daten von Personen, gegen die sie erwägt, allenfalls ein Straf- und je nach dem zu einem späteren Zeitpunkt auch ein Zivilverfahren zu ergreifen. Zum Zeitpunkt der Datenbearbeitung weiss sie indessen nicht, gegen wen sich ein allfälliges Verfahren richten wird. Wenn aber noch nicht einmal die Verfahrensgegenseite bekannt ist, es gar noch nicht fest steht, ob überhaupt je ein Straf- oder Zivilverfahren eröffnet werden wird, kann nicht von einem hängigen Verfahren gesprochen werden. In diese Richtung weist denn auch die Praxis im Zusammenhang mit Strafverfahren: Während gerichtspolizeiliche Ermittlungsverfahren, wenn auch nicht zwingend, als hängige Strafverfahren angesehen und vom Geltungsbereich des DSG ausgeschlossen werden können, werden Präventivermittlungen im Polizeibereich, das heisst Ermittlungen vor einer bevorstehenden Gefahr oder Straftat, nicht von der Ausnahme von Art. 2 DSG erfasst (vgl. Urteil der Eidgenössischen Datenschutzkommission [EDSK] vom 10. Juli 1997, VPB 62.56, E. III/b/3; ROSENTHAL/JÖHRI, a.a.O., Rz. 39 zu Art. 2 DSG; Maurer-Lambrou/Kunz, a.a.O., Rz. 31 zu Art. 2 DSG; Botschaft zum DSG, BBl 1988 II, S. 443). Im vorliegenden Fall gilt dies umso mehr, als - wie sich die Beklagte in der Duplik vernehmen lässt - nicht in jedem Fall ein Prozess angestrengt werden soll, sondern die Daten teilweise bloss zu statistischen Zwecken gesammelt werden, damit die betroffenen Urheberrechtsinhaber Anhaltspunkte erlangen, ob und in welchem Ausmass ihre Werke illegal gehandelt werden. In einem solchen Fall, in dem es gar nie zu einem Verfahren kommt, kann erst recht nicht die Rede von einem hängigen Verfahren sein. Die von der Beklagten gestützt auf DROESE dargelegte Ansicht erscheint allenfalls vertretbar, wenn bereits bekannt ist, wer auf der Prozessgegenseite steht, und es lediglich darum geht, konkrete Beweise zu sammeln. Soll aber wie vorliegend überhaupt erst die anzuzeigende oder zu beklagende Person gefunden werden, ginge es zu weit, die Hängigkeit eines Verfahrens bereits auf diesen Zeitraum auszudehnen mit der Folge, dass das DSG nicht anwendbar wäre. Ein Ausschluss der Anwendbarkeit des Gesetzes gestützt auf Art. 2 Abs. 2 Bst. c DSG rechtfertigt sich nur dann, wenn prozessrechtliche Normen zum Schutz der Persönlichkeit der Betroffenen Platz greifen (vgl. oben E. 3.2.2.). Anders entscheiden hiesse, für Sachverhalte wie den vorliegenden eine nicht hinzunehmende Rechtsschutzlücke zu schaffen.

E. 3.3

Die von der Beklagten vorgenommene Bearbeitung von Personendaten kann folglich nicht als Teil eines hängigen Verfahrens bezeichnet werden. Die Ausnahmebestimmung von Art. 2 Abs. 2 Bst. c DSG kommt daher nicht zur Anwendung und der Geltungsbereich des DSG wird in sachlicher Hinsicht nicht ausgeschlossen.

E. 4.1

Die Beklagte macht weiter geltend, sowohl die Urheberrechtsinhaber als auch die Inhaber der ermittelten IP-Adressen seien stets im Ausland domiziliert, weshalb das DSG nicht zur Anwendung komme.

E. 4.2

Das DSG enthält keine ausdrücklichen Bestimmungen zu seinem räumlichen Geltungsbereich. Auf die Vorschriften mit öffentlich-rechtlichem Charakter ist daher das Territorialitätsprinzip anwendbar (ULRICH HÄFELIN/GEORG MÜLLER/FELIX UHLMANN, Allgemeines Verwaltungsrecht, 5. Aufl., Zürich/Basel/Genf 2006, Rz. 355 ff.). Andernfalls würden die betroffenen Personen ihren datenschutzrechtlichen Schutz verlieren, ohne in den Genuss der prozessrechtlichen Schranken der Informationsbeschaffung zu gelangen, was dem Gesetzeszweck von Art. 2 Abs. 2 Bst. c DSG gerade widersprechen würde. Das DSG ist folglich nur auf Sachverhalte anwendbar, die sich in der Schweiz zutragen, wobei an den Ort der Bearbeitung der Personendaten angeknüpft wird. Unter die Bearbeitung von Personendaten fällt auch deren Bekanntgabe ins Ausland (vgl. ANDRÉ THALMANN, Zur Anwendung des schweizerischen Datenschutzgesetzes auf internationale Sachverhalte, Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht [sic!], 2007, S. 341 f.).

E. 4.3

Die Beklagte ist eine Aktiengesellschaft mit Sitz in Steinhausen im Kanton Zug. Sie nimmt ihre Geschäftstätigkeit an ihrer Niederlassung in der Schweiz vor, so dass eine Datenbearbeitung in der Schweiz stattfindet. Demnach ist vorliegend auch der räumliche Geltungsbereich des DSG gegeben.

E. 5

Das DSG ist folglich in sachlicher wie auch in räumlicher Hinsicht auf den vorliegenden Sachverhalt anwendbar und damit ist auch die Kompetenz des EDÖB zum Erlass von Empfehlungen und deren Weiterziehung an das Bundesverwaltungsgericht grundsätzlich gegeben.

E. 5.1.1

Eine weitere Voraussetzung zur Abgabe einer Empfehlung durch den EDÖB ist das Vorliegen eines Systemfehlers im Sinne von Art. 29 Abs. 1 Bst. a DSG. "Systemfehler" bedeutet in diesem Zusammenhang die Eignung, eine grössere Anzahl von Personen in ihrer Persönlichkeit zu verletzen (vgl. ROSENTHAL, a.a.O., Rz. 11 zu Art. 29 DSG; René Huber, in: Maurer-Lambrou/Vogt [Hrsg.], a.a.O., Rz. 6 ff. zu Art. 29 DSG; Urteil der EDSK vom 15. April 2005, VPB 69.106, E. 3.2). Kann die fragliche Datenbearbeitung potentiell zur Schädigung einer grösseren Anzahl Betroffener führen, ist die Schwelle der "grösseren Anzahl" bereits beim Vorliegen einiger weniger Vorfälle erreicht (Huber, a.a.O., Rz. 10 f. zu Art. 29 DSG).

E. 5.1.2

Die Beklagte bearbeitet Daten von Personen, die in P2P-Netzwerken urheberrechtlich geschützte Werke anbieten. Wie sie selber ausführt, sind Urheberrechtsverletzungen weit verbreitet und kommen häufig vor. Folglich kann das Sammeln solcher Daten als geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen, bezeichnet und - sollten sich die Vorbringen des Klägers als zutreffend erweisen - das Vorliegen eines Systemfehlers im Sinne von Art. 29 Abs. 1 Bst. a DSG bejaht werden.

E. 5.2

Der Kläger hat seine Rechtsbegehren, das Haupt- wie die Eventualbegehren, klar formuliert und die Tatsachen zu deren Begründung sowie die entsprechenden Beweismittel hinreichend dargestellt. Der Begleitbrief zur Klage ist datiert und die Klageschrift unterschrieben. Die Formvorschriften an die Klageschrift gemäss Art. 23 des Bundesgesetzes vom 4. Dezember 1947 über den Bundeszivilprozess (BZP, SR 273) sind somit eingehalten und das Begehren der Beklagten, die Klageschrift zur Nachbesserung zurückzuweisen, ist abzuweisen. Auf die frist- und formgerecht eingereichte Klage ist daher einzutreten.

E. 6

Das Verfahren richtet sich gemäss Art. 44 Abs. 1 VGG grundsätzlich nach den Art. 3 - 73 sowie 79 - 85 BZP. Obwohl im Bundeszivilprozess der Richter sein Urteil grundsätzlich nur auf Tatsachen gründen darf, die im Verfahren geltend gemacht worden sind (Art. 3 Abs. 2 BZP), gilt vor Bundesverwaltungsgericht infolge der spezialgesetzlichen Bestimmung von Art. 44 Abs. 2 VGG der Grundsatz der Sachverhaltsabklärung von Amtes wegen. Art. 3 Abs. 2 BZP bestimmt, dass der Richter nicht über die Rechtsbegehren der Parteien hinausgehen darf. In einem Klageverfahren wie dem vorliegenden hat die Dispositionsmaxime somit grössere Bedeutung als im Beschwerdeverfahren vor Bundesverwaltungsgericht. Der Streitgegenstand wird ausschliesslich durch die gestellten Anträge (und allenfalls der entsprechenden Begründung) definiert. Einer Partei darf nicht mehr oder nichts anderes zugesprochen werden, als sie beantragt hat (BVGE 2008/16 E. 2.2; ANDRÉ MOSER/MICHAEL BEUSCH/LORENZ KNEUBÜHLER, Prozessieren vor dem Bundesverwaltungsgericht, Basel 2008, Rz. 5.14; ALFRED KÖLZ/JÜRG BOSSHART/MARTIN RÖHL, Kommentar zum Verwaltungsrechtspflegegesetz des Kantons Zürich, 2. Aufl., Zürich 1999, Rz. 7 zu § 85).

E. 7

Nachfolgend ist die Rechtmässigkeit der Bearbeitung der Personendaten durch die Beklagte zu prüfen. Zunächst stellt sich die Frage, ob die von der Beklagten vorgenommene Datenbearbeitung eine Persönlichkeitsverletzung im Sinne von Art. 12 DSG darstellt. Wer Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen (Art. 12 Abs. 1 DSG). Insbesondere dürfen Personendaten nicht entgegen den Grundsätzen von Art. 4 DSG oder ohne Rechtfertigungsgrund gegen den ausdrücklichen Willen der betroffenen Person bearbeitet werden (Art. 12 Abs. 2 Bst. a und b DSG). In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 12 Abs. 3 DSG). Art. 4 DSG verlangt, dass Personendaten nur rechtmässig bearbeitet werden dürfen (Abs. 1), dass ihre Bearbeitung nach Treu und Glauben zu erfolgen hat und verhältnismässig sein muss (Abs. 2), dass Daten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Abs. 3) und dass die Beschaffung der Daten und insbesondere der Zweck ihrer Bearbeitung für die betroffene Person erkennbar sein muss (Abs. 4).

E. 8.1

Der Kläger wirft der Beklagten vor, automatisiert und proaktiv Personendaten ohne Wissen der Betroffenen zu bearbeiten. In der Schweiz existiere derzeit keine spezifische gesetzliche

Grundlage, welche die systematische Erhebung von Personendaten in P2P-Netzwerken durch Privatpersonen erlaube oder verbiete. Daher sei die Rechtmässigkeit der Datenbearbeitung durch die Beklagte grundsätzlich nach dem DSG zu beurteilen. Es sei indessen erforderlich, dass eine solche Datenbearbeitung gesetzlich geregelt werde, denn diese habe eine grosse Reichweite und tangiere die Persönlichkeitsrechte einer Vielzahl betroffener Personen. Es müssten Kriterien gefunden werden, welche die Zulässigkeit der erhobenen Daten als Beweismittel im Rahmen von rechtlichen Verfahren regeln würden, und es müsse gewährleistet sein, dass die überwachende Person kein Interesse an einer zu weitgehenden Überwachung habe und die Unabhängigkeit garantiert sei. Des Weiteren sei die Identifikation einer hinter einer IP-Adresse stehenden Person durch das Fernmeldegeheimnis gemäss Art. 43 des Fernmeldegesetzes vom 30. April 1997 (FMG, SR 784.10) untersagt. Im zivilrechtlichen Bereich bestehe zurzeit keine Möglichkeit, dieses zu durchbrechen. Einzig auf dem Weg der Strafverfolgung könne das Fernmeldegeheimnis durchbrochen werden. Zur Bekämpfung von Urheberrechtsverletzungen im Rahmen von P2P-Netzwerken müsse daher eine gesetzliche Grundlage geschaffen werden, um die Möglichkeit der Identifikation der betroffenen Personen zu regeln.

E. 8.2

Die Beklagte bestreitet, systematisch und proaktiv Verbindungsdaten im Internet zu sammeln. Sie sammle lediglich auf konkreten Auftrag eines Urheberrechtsinhabers hin, der um Urheberrechtsverletzungen bei seinen Werken wisse oder solche vermute, technische Informationen und gebe diese anschliessend an den Auftraggeber weiter. Gesetzliche Grundlage zur Durchbrechung des Fernmeldegeheimnisses bilde vorliegend das jeweilige Strafverfahren bzw. das entsprechende Strafprozessrecht. Art. 14 BÜPF regle detailliert, welche Auskünfte über Fernmeldeanschlüsse die Anbieterinnen von Fernmeldediensten dem Dienst liefern müssten (Abs. 1) und an wen der Dienst die Auskünfte ausschliesslich erteilen dürfe (Abs. 2). Art. 14 Abs. 4 BÜPF regle ausdrücklich, dass die Internet-Anbieterin im Falle einer Straftat über das Internet verpflichtet sei, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen würden. Damit könne nur gemeint sein, dass die Anbieterin mitteilen müsse, wer ihre IP-Adresse zur fraglichen Zeit benützt habe, und sie die zugehörigen Eckdaten liefern müsse. Diese Auskunftspflicht gelte unabhängig davon, ob die Daten überhaupt unter das Fernmeldegeheimnis fielen. Es sei das gute Recht der Urheberrechtsinhaber, bei Verdacht auf Urheberrechtsverletzungen strafrechtlichen Schutz in Anspruch zu nehmen. Die Strafverfolgungsbehörden würden im Ermittlungsverfahren zunächst abklären, ob genügend Anhaltspunkte für die Durchführung eines Verfahrens gegeben seien. Diese Anhaltspunkte oder Indizien stelle die Beklagte für die Urheberrechtsinhaber bereit, indem sie entsprechende, frei zugängliche und von den P2P-Netzwerkteilnehmern freiwillig offenbarte technische Informationen sammle. Zur Geltendmachung von Zivilansprüchen, die gegen einen mutmasslichen Verletzer einer Straftat entstünden, stehe es dem Geschädigten denn auch offen, einen Adhäsionsprozess zu führen.

E. 8.3.1

Art. 4 Abs. 1 DSG enthält die an und für sich selbstverständliche Aussage, dass Personendaten nur rechtmässig beschafft werden dürfen. Obwohl der Wortlaut nur von "beschaffen" spricht, gilt der Grundsatz für jede Bearbeitung von Daten. Eine Datenerhebung ist immer dann rechtswidrig, wenn ein Verstoss gegen eine Rechtsnorm vorliegt. Des Weiteren ist sie rechtswidrig, wenn eine Verwendung der Daten durch den

Betroffenen generell bzw. zu einem bestimmten Zweck untersagt wurde oder der eigentliche Zweck bewusst wahrheitswidrig hinter anderen scheinbar seriösen Zwecken versteckt wird (Urs Maurer-Lambrou/Andrea Steiner, in: Maurer-Lambrou/Vogt [Hrsg.], a.a.O., Rz. 5 f. zu Art. 4 DSG).

E. 8.3.2

In der Schweiz besteht zurzeit keine gesetzliche Grundlage, die das Erfassen und Weiterleiten von Personendaten in P2P-Netzwerken regelt. Die Datenerfassung ist demnach nicht ausdrücklich verboten. Die Regelung von Art. 14 BÜPF, auf die sich die Beklagte stützt, begründet zwar in Abweichung vom Fernmeldegeheimnis gemäss Art. 43 FMG eine Auskunftspflicht über IP-Adressen, wenn eine Straftat über das Internet begangen wurde. Sie betrifft aber nicht den vorliegend zu beurteilenden Fall, sondern würde allenfalls in einem weiteren Schritt, im Rahmen einer durch die Behörde erfolgenden Datenbearbeitung, zur Anwendung gelangen. Dagegen ist für das Vorgehen der Beklagten keine ausdrückliche gesetzliche Grundlage erforderlich, da sich diese im privatrechtlichen Umfeld betätigt und ihr Handeln nicht etwa als staatliches zu qualifizieren ist. Das Rechtmässigkeitsprinzip gemäss Art. 4 Abs. 1 DSG wird durch das Vorgehen der Beklagten somit nicht verletzt.

E. 9.1

Im Weiteren macht der Kläger geltend, das Vorgehen der Beklagten, das Fernmeldegeheimnis mittels Strafverfahren zu umgehen, widerspreche dem Prinzip von Treu und Glauben und sei rechtsmissbräuchlich. Einerseits liege dabei ein Institutionenmissbrauch vor, da die Urheberrechtsinhaber meist nicht einmal das Ende der Strafuntersuchung abwarten würden, um ihre Zivilansprüche anzubringen. Andererseits würden diese in keiner Weise den Beweis erbringen, dass ihnen durch das Anbieten eines urheberrechtlich geschützten Werks ein Schaden entstanden sei. Ein solcher könne denn auch nicht beziffert werden. Die Urheberrechtsinhaber würden einfach einen hypothetischen Schaden von mehreren Tausend Euro annehmen. Zum Zeitpunkt der Strafanzeige sowie der Akteneinsichtnahme sei zudem noch nicht klar, ob überhaupt eine relevante strafbare Handlung vorliege. Für den mutmasslichen Urheberrechtsverletzer sei während des Download-Prozesses nämlich nicht erkennbar, dass Teile des Werks im P2P-Netzwerk angeboten würden. Daher könne nicht grundsätzlich von einer vorsätzlichen Urheberrechtsverletzung ausgegangen werden. Schliesslich würden sich das Zivilverfahren sowie die von den Urheberrechtsinhabern vorgenommenen Massnahmen nicht notwendigerweise gegen den Urheberrechtsverletzer, sondern gegen den gutgläubigen Inhaber des Internetanschlusses richten. Zusammengefasst verstosse die von den Urheberrechtsinhabern durchgeführte Datenbearbeitung gegen das Prinzip von Treu und Glauben, solange keine gesetzliche Grundlage existiere, welche eine Weitergabe von personenbezogenen Verkehrsdaten und deren Verwendung zur zivilrechtlichen Verfolgung von Urheberrechtsverletzungen legitimiere.

E. 9.2

Die Beklagte hebt demgegenüber hervor, vorliegend bilde das jeweilige Fernmelde- und Strafprozessrecht in den fraglichen Ländern die entsprechende gesetzliche Grundlage. Die Identifikation von IP-Adressen erfolge ausnahmslos im Rahmen von Strafverfahren gemäss gesetzlicher Grundlage. Dabei finde keine Umgehung statt, sondern die Urheberrechtsinhaber würden lediglich ihre Parteirechte im Strafverfahren ausüben. Ihr Vorgehen sei vergleichbar mit demjenigen des geschädigten Strassenverkehrsteilnehmers,

der über die amtliche Kontrollschildnummer gegen den Halter eines unfallverursachenden Fahrzeugs strafrechtlich vorgehe. Im Zivilprozess sei die Verwendung von den Untersuchungsakten entnommenen Beweisen grundsätzlich zulässig. Als absolutes Recht könne das Urheberrecht wie auch das Eigentumsrecht jederzeit gegenüber jedem Dritten durchgesetzt werden. Ausserdem sei es bei ausservertraglichen Schädigungen keine Seltenheit, dass im Zeitpunkt der Geltendmachung zivilrechtlicher Ansprüche Ausmass und Höhe des eingetretenen Schadens noch nicht feststünden. Der nicht ziffernmässig nachweisbare Schaden werde nach richterlichem Ermessen geschätzt. Zudem würden zivilrechtliche Forderungen keine strafrechtliche Verurteilung voraussetzen. Schliesslich könnten die IP-Adressinhaber nicht als gutgläubig bezeichnet werden. Um an einem P2P-Netzwerk teilnehmen zu können, müsse nämlich auf dem fraglichen Rechner die entsprechende Spezialsoftware installiert sein.

E. 9.3.1

Das DSG unterstellt die Bearbeitung von Personendaten dem Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG). Die Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV, SR 101) erhebt in Art. 5 Abs. 3 den Grundsatz von Treu und Glauben zum Verfassungsprinzip, das auch unter Privaten unmittelbar anwendbar ist. Dieser Grundsatz gilt im Privatrechtsbereich (Art. 2 des Schweizerischen Zivilgesetzbuchs vom 10. Dezember 1907 [ZGB, SR 210]) wie auch in verwaltungsrechtlichen Verhältnissen. Er gebietet ein loyales und vertrauenswürdiges Verhalten im Rechtsverkehr. Die Beteiligten dürfen sich nicht widersprüchlich und auch sonst nicht missbräuchlich verhalten (Yvo Hangartner, in: Die schweizerische Bundesverfassung, Kommentar, a.a.O., N. 41-43 zu Art. 5 BV). Im Geschäftsverkehr hat das Gebot von Treu und Glauben eine herausragende Bedeutung; es gehört zum Kreis der universell anerkannten Rechtsgüter, deren Schutz der positive «Ordre public» dient (BGE 128 III 201 E. 1.c). Dem Prinzip von Treu und Glauben kommt gerade bei der Datenbeschaffung besondere Wichtigkeit zu. Daten sollen nicht in einer Art erhoben werden, mit der die betroffene Person nicht rechnen musste und mit der sie nicht einverstanden gewesen wäre. Wider Treu und Glauben handelt namentlich, wer Daten durch absichtliche Täuschung beschafft, weil er beispielsweise die betroffene Person über seine Identität oder den Zweck seiner Bearbeitung falsch informiert, oder wer heimlich Daten beschafft, ohne dabei eine Rechtsnorm zu verletzen (vgl. Botschaft zum DSG, BBl 1988 II, S. 449). Aus dem Grundsatz von Treu und Glauben ist auch die Anforderung abzuleiten, dass eine Datenbearbeitung transparent erfolgen muss, das heisst grundsätzlich für die betroffene Person erkennbar sein muss (Maurer-Lambrou/ Steiner, a.a.O., Rz. 7 f. zu Art. 4 DSG).

E. 9.3.2

Im Zusammenhang mit der Prüfung einer Verletzung des Grundsatzes von Treu und Glauben ist daher auch die vom Kläger gerügte Verletzung des Erkennbarkeitsprinzips zu behandeln. Der Kläger macht geltend, dieses sei verletzt, weil die von der Beklagten durchgeführte Datenbearbeitung heimlich stattfinde und weder für den Urheberrechtsverletzer noch für den Inhaber des Internetanschlusses erkennbar sei. Würden die Daten als besonders schützenswerte Personendaten im Sinne von Art. 3 Bst. c DSG qualifiziert, käme der Beklagten sogar eine gesteigerte Informationspflicht zu, wonach die Einwilligung der betroffenen Person nach angemessener Information ausdrücklich zu erfolgen habe (Art. 4 Abs. 5 DSG).

E. 9.3.3

Die Beklagte weist darauf hin, dass P2P-Netzwerkteilnehmer im Programm ausdrücklich darauf aufmerksam gemacht würden, dass sie sich in einem öffentlichen Bereich befänden. Nicht nur P2P-Netzwerke, sondern das Internet allgemein gälten als öffentlicher Bereich. Zudem zeichne sie, die Beklagte, lediglich ihre eigenen technischen Informationen auf. Dies geschehe nicht heimlich. Es handle sich vielmehr um ein übliches Sicherungs- resp. Backup-Prinzip.

E. 9.3.4

Vor dem Hintergrund des Vertrauensprinzips erscheint das Vorgehen der Beklagten in der Tat diskutabel. So sammelt diese Daten über P2P-Netzwerkteilnehmer, die sie an ihre Auftraggeber weitergibt. Die Datenbeschaffung geschieht hierbei im Regelfall ohne Wissen der betroffenen Personen, das heisst auch, dass sie für diese nicht erkennbar ist. Es dürfte daher regelmässig eine Verletzung des Erkennbarkeitsprinzips vorliegen. Zugleich ist aber auch zu berücksichtigen, dass die Beklagte lediglich Daten von P2P-Netzwerkteilnehmern erfasst, die sich vermutungsweise urheberrechtlich strafbar gemacht haben. Die erhobenen Daten werden sodann verwendet, um gegen die vermuteten Verletzer rechtlich vorzugehen. Angesichts der heutigen gesetzlichen Lage bleibt den Urheberrechtsinhabern kaum eine andere rechtliche Möglichkeit, gegen Urheberrechtsverletzungen vorzugehen. Es kann daher nicht erwartet werden, dass Urheberrechtsverletzungen stillschweigend hingenommen werden und die Verletzer unbescholten davon kommen, wenn - im rechtlich zulässigen Rahmen - Massnahmen dagegen ergriffen werden können. Darauf wird bei der Prüfung des Vorliegens von Rechtfertigungsgründen vertieft einzugehen sein (vgl. unten E. 12). Das Vorgehen der Beklagten als Reaktion auf vorangegangene oder zumindest vermutete Rechtsverletzungen erscheint daher als mit dem Grundsatz von Treu und Glauben vereinbar.

E. 9.3.5

Die Beklagte bezeichnet P2P-Netzwerke wie auch das Internet im Allgemeinen als öffentlichen Bereich. Sollte sie sich damit auf Art. 12 Abs. 3 DSG berufen wollen, wonach in der Regel keine Persönlichkeitsverletzung vorliegt, wenn eine Person ihre Daten mit Wissen und Willen allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (vgl. Rosenthal, a.a.O., Rz. 54 zu Art. 12 DSG), ist Folgendes entgegen zu halten: Selbst wenn das Internet bis zu einem gewissen Grad als öffentlicher Bereich qualifiziert werden könnte, was an dieser Stelle indessen nicht abschliessend beurteilt werden muss, bedeutet die Nutzung des Internets nicht, dass damit ohne Weiteres eigene Daten sämtlichen Internetnutzern zugänglich gemacht werden sollen. Nur solange sich eine Bearbeitung allgemein zugänglicher Personendaten im Rahmen des aus den Umständen ersichtlichen Veröffentlichungszwecks bewegt, ist sie nicht persönlichkeitsverletzend (Corrado Rampini, in: Maurer-Lambrou/Vogt [Hrsg.], a.a.O., Rz. 18 zu Art. 12 DSG). Die IP-Adresse wird im Normalfall nicht willentlich bekannt gegeben und schon gar nicht zum Zweck der Einsicht oder gar Bearbeitung durch Dritte. Vielmehr steckt ein technischer Prozess dahinter. Es dürften sich zudem auch nicht sämtliche Internetnutzer bewusst sein, überhaupt über eine für Dritte erkennbare IP-Adresse zu verfügen resp. deren Spuren im Internet zu hinterlassen. Von allgemein zugänglich gemachten Daten kann daher nicht ausgegangen werden.

E. 9.3.6

Zusammengefasst dürfte bei der Datenbearbeitung durch die Beklagte regelmässig das Erkennbarkeitsprinzip verletzt sein. Angesichts der Umstände, die die Beklagte erst zur Datensammlung bewegen, hält diese aber vor dem Grundsatz von Treu und Glauben stand. Da es sich nicht um eine Bearbeitung besonders schützenswerter Personendaten handelt (vgl. oben E. 2.2.5), bedarf es entgegen dem Vorbringen des Klägers keiner ausdrücklichen Einwilligung des Betroffenen.

E. 10.1

Der Kläger beanstandet des Weiteren eine Verletzung des Zweckmässigkeitsprinzips. Die von der Beklagten durchgeführte Datenbearbeitung zum Zweck der Feststellung, Identifikation und rechtlichen Verfolgung der betroffenen Person erfolge heimlich, das heisst ohne Wissen dieser Person. Der verfolgte Zweck der Datenbearbeitung sei für diese auch nicht aus den Umständen ersichtlich. Somit bearbeite die Beklagte die Daten ohne Einwilligung des Anbieters des Werkes und zu einem Zweck, der weder bei der Beschaffung angegeben worden bzw. aus den Umständen ersichtlich noch gesetzlich vorgesehen sei. Zudem biete die Software, welche in der Regel in P2P-Netzwerken zum Download von Dateien verwendet werde, regelmässig während des Download-Prozesses die heruntergeladenen Teile des Werkes automatisch wieder auf dem P2P-Netzwerk an. Dies erfolge ohne Zutun und in vielen Fällen sogar ohne Wissen des jeweiligen Nutzers.

E. 10.2

Die Beklagte weist darauf hin, lediglich im Auftrag der Urheberrechtsinhaber auf bereits bestehende widerrechtliche Angebote geschützter Werke in P2P-Netzwerken zu reagieren. Die vorliegend umstrittene Datenbearbeitung betreffe nur denjenigen P2P-Netzwerkteilnehmer, der die konkreten urheberrechtlich geschützten Werke anbieten würde. Dazu müsse eine Spezialsoftware auf dem entsprechenden Rechner installiert sein. Die Frage einer strafrechtlich relevanten Beteiligung des IP-Adressinhabers, der allenfalls nicht mit dem Urheberrechtsverletzer identisch sei, müsse von der zuständigen Strafuntersuchungsbehörde im ordentlichen Strafverfahren abgeklärt werden.

E. 10.3.1

Das in Art. 4 Abs. 3 DSG enthaltene Zweckmässigkeitsprinzip besagt, dass Personendaten nur für den Zweck bearbeitet werden dürfen, welcher bei der Beschaffung angegeben worden ist oder der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Der Verwendungszweck der Daten muss bereits bei der Datenbeschaffung angegeben worden sein oder sonst feststehen. Die betroffene Person muss nicht hinnehmen, dass über sie Daten ohne nähere Zweckbestimmung auf Vorrat erhoben werden (Rosenthal, a.a.O., Rz. 20 zu Art. 4 DSG; Maurer-Lambrou/Steiner, a.a.O., Rz. 13 f. zu Art. 4 DSG).

E. 10.3.2

Die Beklagte spürt in P2P-Netzwerken systematisch Werke von Urheberrechtsinhabern auf, die sie, die Beklagte, hiermit beauftragt haben. Findet sie ein solches Werk, zeichnet sie die Daten, insbesondere die IP-Adresse, des Anbieters auf und leitet diese an den Auftraggeber weiter. Die Suche nach den urheberrechtlich geschützten Werken und die Aufzeichnung der entsprechenden Daten geschieht ohne Wissen der betroffenen Adressinhaber. Selbst wenn, wie die Beklagte behauptet, vereinzelt darauf aufmerksam gemacht werden sollte, dass "Anti-P2P-Firmen Daten loggen", kann dabei keineswegs von einer Angabe des Datenbeschaffungszwecks durch die Bearbeiterin gesprochen werden. Das Vorgehen der Beklagten schliesst aus, dass dem IP-Adressinhaber im Moment der Beschaffung

angegeben wird, wozu seine Daten gespeichert werden. Der Bearbeitungszweck ist auch aus den Umständen der Datensammlung nicht ersichtlich. Im Gegenteil beruht das Vorgehen der Beklagten gerade darauf, dass die Benutzer des P2P-Netzwerks ihre Absichten nicht frühzeitig erkennen, würde doch sonst die Ermittlung der betreffenden Adressen regelmässig verunmöglicht. Die Beklagte verletzt das Zweckmässigkeitsprinzip daher regelmässig.

E. 11.1

Schliesslich wird die Verletzung des Grundsatzes der Verhältnismässigkeit vorgebracht. Der Kläger unterscheidet zwischen der Geltendmachung von Schadenersatzforderungen und der strafrechtlichen Verfolgung der Urheberrechtsverletzer. Zur Geltendmachung von Schadenersatzforderungen sei es notwendig, den Schädiger zu identifizieren und den entstandenen Schaden zu beziffern. Wenn allerdings im zivilrechtlichen Bereich keine Möglichkeit bestehe, das Fernmeldegeheimnis zu durchbrechen, sei eine Identifizierung des Schädigers nicht möglich und die Datensammlung folglich nicht notwendig resp. geeignet. Sollte eine zivilrechtliche Grundlage zur Durchbrechung des Fernmeldegeheimnisses bestehen, wäre die Datensammlung dennoch keine geeignete Massnahme, da der erlittene Schaden regelmässig nicht ermittelt werden könne, was für ein erfolgreiches Zivilverfahren aber erforderlich wäre. Im Hinblick auf ein Strafverfahren könne die von der Beklagten durchgeführte Datenbearbeitung zwar als geeignet bezeichnet werden, jedoch genüge das Interesse an der Bekämpfung der Piraterie in P2P-Netzwerken nicht, um das Vorgehen der Beklagten zu rechtfertigen. Für eine systematische, vollständige und dauerhafte Überwachung von P2P-Netzwerken müsse eine gesetzliche Grundlage existieren, die einen Eingriff in die durch das Fernmeldegeheimnis geschützte Persönlichkeit der Betroffenen rechtfertige.

E. 11.2

Die Beklagte führt aus, neben privaten würden auch öffentliche Interessen, unter anderem das Urheberrecht als zivil- und strafrechtlich geschütztes Rechtsgut, ihr Sammeln technischer Informationen rechtfertigen. Die Urheberrechtsinhaber wollten nicht nur ihren Schaden ersetzt erhalten und die Bestrafung der Urheberrechtsverletzer erwirken, sondern beispielsweise auch vorsorgliche zivilprozessuale Massnahmen bei drohenden Verletzungen durchsetzen. Die Sammlung technischer Informationen sei die einzige Möglichkeit der Urheberrechtsinhaber, zivilrechtliche Forderungen überhaupt geltend machen zu können. Die Einleitung eines Zivilverfahrens betreffend Unterlassung und Schadenersatz sei ohne Kenntnis des Namens des tatsächlichen oder mutmasslichen Verletzers nicht möglich, weshalb die Urheberrechtsinhaber gezwungen seien, zunächst ein Strafverfahren gegen Unbekannt einzuleiten. Die Datensammlung durch die Beklagte sei daher sowohl geeignet als auch verhältnismässig. Die Parteirechte des Opfers im Strafverfahren seien gerade um der Durchsetzung seiner Zivilansprüche willen festgesetzt worden. Die Persönlichkeit der betroffenen Personen nach Massgabe der anwendbaren gesetzlichen Grundlagen zu schützen, sei Sache der zuständigen Untersuchungsbehörden.

E. 11.3

Auch dem Grundsatz der Verhältnismässigkeit kommt Verfassungsrang zu (Art. 5 Abs. 2 BV). Ein Verhalten entspricht dann dem Verhältnismässigkeitsprinzip, wenn die Massnahme geeignet ist, das im öffentlichen Interesse angestrebte Ziel zu erreichen (Zwecktauglichkeit), und sie diejenige ist, welche die privaten Interessen am meisten schont

(geringst möglicher Eingriff). Schliesslich muss sie ein vernünftiges Verhältnis zwischen dem angestrebten Ziel und dem Eingriff, den sie für den betroffenen Privaten bewirkt, wahren (Häfelin/Müller/ Uhlmann, a.a.O., Rz. 581 ff.). Aus dem allgemein geltenden Verhältnismässigkeitsgrundsatz lässt sich für die Datenbearbeitung ableiten, dass ein Datenbearbeiter nur diejenigen Daten beschaffen und bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt und die mit Blick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen (Rosenthal, a.a.O., Rz. 20 zu Art. 4 DSG; Maurer-Lambrou/Steiner, a.a.O., Rz. 9 ff. zu Art. 4 DSG).

E. 11.4

Ob die Datenbearbeitung der Beklagten vor dem Verhältnismässigkeitsprinzips stand hält, braucht an dieser Stelle nicht überprüft zu werden. Die vorstehenden Erwägungen haben gezeigt, dass die Beklagte durch das Sammeln von Daten in P2P-Netzwerken sowohl das Zweckmässigkeitsprinzip gemäss Art. 4 Abs. 3 DSG als auch das Erkennbarkeitsprinzip gemäss Art. 4 Abs. 4 DSG verletzt, mithin eine Persönlichkeitsverletzung vorliegt. Fraglich ist aber, ob das Vorgehen der Beklagten im Sinne von Art. 13 DSG gerechtfertigt ist. Bei der Überprüfung der Rechtfertigungsgründe ist unter anderem auch das Vorliegen überwiegender privater oder öffentlicher Interessen abzuklären. Da in diese Erwägungen dieselben Überlegungen einfliessen wie bei der Verhältnismässigkeitsprüfung, ist hierauf im Folgenden einzugehen.

E. 12

Die Datenbearbeitung durch die Beklagte könnte folglich aufgrund eines Rechtfertigungsgrundes im Sinne von Art. 13 DSG zulässig sein. Danach ist eine Verletzung der Persönlichkeit widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (Art. 13 Abs. 1 DSG).

E. 12.1

Die Einwilligung erfordert, dass die betroffene Person in den Grundzügen über Gegenstand, Zweck und Umfang der beabsichtigten Datenbearbeitung aufgeklärt sein muss, damit sie die Konsequenzen der Einwilligung abschätzen kann. Eine stillschweigende Zustimmung darf nur angenommen werden, wenn und soweit beispielsweise ein Vertrag die Bearbeitung von Personendaten zwingend mit sich bringt und mit Vertragsschluss stillschweigend die Zustimmung zur erforderlichen Datenbearbeitung erteilt wurde. Grosse Zurückhaltung ist bei einer mutmasslichen, hypothetischen Einwilligung geboten. Eine solche wird in der Lehre nur in Notsituationen, wie etwa bei einem bewusstlosen Patienten, als zulässig erachtet (vgl. Rampini, a.a.O., Rz. 1 ff. zu Art. 13 DSG). Von einer Einwilligung der betroffenen Person kann im vorliegenden Fall nicht ausgegangen werden, zumal die Datenbearbeitung in der Regel ohne deren Wissen erfolgt, eine Einwilligung daher von vornherein ausgeschlossen ist. Für eine mutmassliche Einwilligung ist bei der vorliegenden Ausgangslage kein Raum.

E. 12.2

Eine ausdrückliche gesetzliche Grundlage, die Bearbeitungsrechte oder -pflichten festlegen würde, ist zurzeit nicht vorhanden.

E. 12.3

Zu prüfen bleibt daher einzig, ob ein überwiegendes privates oder öffentliches Interesse die Datenbearbeitung zu rechtfertigen vermag.

E. 12.3.1

Als überwiegende private Bearbeitungsinteressen kommen in erster Linie die Interessen der bearbeitenden Person, aber auch solche von Dritten in Frage. Vorliegend ist zu berücksichtigen, dass die Beklagte die Daten im Auftrag von Urheberrechtsinhabern sammelt. Sie gilt daher als Dritte im Sinne von Art. 10a DSG und kann dieselben Rechtfertigungsgründe geltend machen wie die Auftraggeber (Art. 10a Abs. 3 DSG; vgl. Rosenthal, a.a.O., Rz. 133 zu Art. 10a DSG). Bei der Interessenabwägung können grundsätzlich alle schützenswerten Interessen an der Datenbearbeitung berücksichtigt werden, das heisst alle Interessen von allgemein anerkanntem Wert. Ob das Interesse schützenswert ist, hängt vom Zweck der Bearbeitung ab (Rosenthal, a.a.O., Rz. 10 zu Art. 13 DSG; Rampini, a.a.O., Rz. 20 ff. zu Art. 13 DSG). Art. 13 Abs. 2 DSG nennt beispielhaft verschiedene Rechtfertigungsgründe; die Aufzählung ist nicht abschliessend. Neben privaten können auch öffentliche Interessen eine Datenbearbeitung rechtfertigen.

E. 12.3.2

Das Urheberrecht ist als absolutes Herrschaftsrecht über einen immateriellen Gegenstand ein Teil der privatrechtlich organisierten Eigentumsordnung und steht als solches unter dem Schutz der Bundesverfassung (vgl. Art. 26 BV). Das Urheberrecht schützt die Nutzung des immateriellen Produkts durch Unberechtigte. Zugleich dient der Schutz auch der Verkehrsfähigkeit des Urheberrechts (MANFRED REHBINDER/ADRIANO VIGANO, Urheberrecht, Kommentar, 3. Aufl., Zürich 2008, Rz. 3 f. zu Art. 1). Die Beklagte beruft sich sowohl auf private wie auch auf öffentliche Interessen (vgl. oben E. 11.2). Als wesentliches Interesse wird dasjenige der Urheberrechtsinhaber an der Durchsetzung der ihnen gegen die Urheberrechtsverletzer zustehenden Ansprüche geltend gemacht. Auf diese Interessen kann sich auch die Beklagte als Beauftragte der Urheberrechtsinhaber berufen. Die Urheberrechtsinhaber werden in ihren Rechten verletzt, wogegen sie sich wehren. Hierzu müssen sie wissen, wer ihre Rechte verletzt hat, damit sie die ihnen gegen diese Personen zustehenden Ansprüche geltend machen können. Die Datenbearbeitung der Beklagten ist geeignet, der Durchsetzung der Rechte und Ansprüche von Urheberrechtsinhabern zu verhelfen. Ohne die Sammlung der technischen Daten, wie insbesondere der IP-Adresse, wäre es für die in ihren Rechten verletzten Urheberrechtsinhaber nicht möglich, die Verletzer zu identifizieren und gegen diese Schadenersatz- wie auch Unterlassungsansprüche geltend zu machen. Ein anderes, milderes Vorgehen, das zum selben Ziel führen würde, ist nicht ersichtlich. Vielmehr sind die Daten gerade objektiv notwendig, um die vermuteten Urheberrechtsverletzer identifizieren und anschliessend gegen diese vorgehen zu können. Demgegenüber erscheint der Eingriff in die Persönlichkeitsrechte der betroffenen Personen nicht ausgesprochen schwerwiegend. Sollten sich die Beweise nicht erhärten, würde ein Strafverfahren - dessen Einleitung als solche zwar zu Unannehmlichkeiten führen kann - eingestellt werden und entsprechende Zivilansprüche würden sich als nicht gerechtfertigt erweisen. Es erscheint bei dieser Ausgangslage weder missbräuchlich noch unverhältnismässig, technische Daten zu sammeln, um mit diesen die Verletzer zu identifizieren. Dabei ist nicht ausser Acht zu lassen, dass es in der Regel der IP-Adressinhaber ist, der zumindest vermutungsweise gegen das Urheberrecht verstossen hat. Gleichzeitig liegt auch die Durchsetzung bestehenden Rechts - des Urheberrechts wie des Strafrechts - im öffentlichen Interesse. Die Interessen

der Urheberrechtsinhaber resp. der Beklagten, aber auch das öffentliche Interesse überwiegen daher insgesamt die Interessen der von der Datenbearbeitung betroffenen Personen. Somit lässt sich festhalten, dass die Beklagte mit ihrem Vorgehen zwar die Persönlichkeit der von der Datenbearbeitung betroffenen Personen verletzt, die Verletzung aber durch überwiegende private und öffentliche Interessen gerechtfertigt und damit nicht widerrechtlich ist. Die Begehren des Klägers sind daher abzuweisen.

E. 13

Die Beklagte beantragt schliesslich, der Kläger sei zu verpflichten, die schweizerische Presse und Öffentlichkeit umfassend und aktiv über das Urteil des Bundesverwaltungsgerichts in der vorliegenden Klagesache zu orientieren. Das Verfahren habe ein weites Echo sowohl in der Presse als auch der übrigen Öffentlichkeit gefunden, weshalb sie, die Beklagte, ein berechtigtes Interesse an der entsprechenden Information besitze. Ob derartige, über die blosse Zurück- oder Abweisung hinausgehende Begehren der Beklagten im Klageverfahren vor dem Bundesverwaltungsgericht überhaupt zulässig sind, kann an dieser Stelle offen gelassen werden, zumal - wie sogleich zu sehen ist - vorliegend ohnehin nicht darauf eingetreten werden kann.

E. 13.1

Gemäss Art. 25a Abs. 1 des Bundesgesetzes vom 20. Dezember 1968 über das Verwaltungsverfahren (VwVG, SR 172.021) kann, wer ein schutzwürdiges Interesse hat, von der Behörde, die für Handlungen zuständig ist, verlangen, dass sie widerrechtliche Handlungen unterlässt, einstellt oder widerruft (Bst. a), die Folgen widerrechtlicher Handlungen beseitigt (Bst. b) oder die Widerrechtlichkeit von Handlungen feststellt (Bst. c). Die Behörde entscheidet durch Verfügung (Abs. 2). Laut der Marginalie zu Art. 25a VwVG geht es um den Erlass einer Verfügung über Realakte. Zweck der Bestimmung ist, Verwaltungshandlungen, die nicht wie Verfügungen der Beschwerde unterliegen, Rechtsschutz zu gewähren. Als Realakte (im weiteren Sinne) gelten unter anderem amtliche Warnungen oder Empfehlungen (Beatrice Weber-Dürler, in: Kommentar zum Bundesgesetz über das Verwaltungsverfahren, Auer/Müller/ Schindler [Hrsg.], Zürich/St.Gallen 2008, Rz. 6 f. zu Art. 25a VwVG).

E. 13.2

Die Beklagte stört sich an der Veröffentlichung der umstrittenen Empfehlung des Klägers vom 9. Januar 2008 auf der Website <www.edoeb.admin.ch> sowie darüber, dass der Kläger Presse und Öffentlichkeit über den Inhalt der Empfehlung informiert habe. Die Handlungen des Klägers sind als Realakte zu qualifizieren. Begehrt die Beklagte Rechtsschutz hiergegen, hat sie sich gemäss Art. 25a VwVG direkt an den EDÖB als zuständige Behörde zu wenden. Dessen Verfügung könnte sie, wenn sie sich nicht mit ihr abfinden sollte, mit Beschwerde anfechten. Es besteht dagegen keine Rechtsgrundlage, die die Zuständigkeit und ein Eingreifen des Bundesverwaltungsgerichts im Sinne des Antrags der Beklagten begründen würde. Auf das Begehren kann daher nicht eingetreten werden.

E. 13.3

Für weitergehende, sich auf das Persönlichkeitsrecht stützende Ansprüche ist das Bundesverwaltungsgericht ebenfalls nicht zuständig; hierzu ist auf die Zivilgerichtsbarkeit zu verweisen.

E. 14

Zusammenfassend ist festzuhalten, dass das Sammeln und Weitergeben von technischen Daten durch die Beklagte eine Bearbeitung von Personendaten im Sinne des DSG darstellt. Das DSG ist daher auf den vorliegenden Fall anwendbar und der EDÖB war zur Abgabe der umstrittenen Empfehlung zuständig. Die Überprüfung der Datenbearbeitung hat gezeigt, dass diese die Persönlichkeit der betroffenen Personen verletzt, da weder das Zweckmässigkeits- noch das Erkennbarkeitsprinzip eingehalten werden. Da indes überwiegende private wie auch öffentliche Interessen die Verletzung rechtfertigen, erweist sich die Persönlichkeitsverletzung nicht als widerrechtlich. Die Klage ist demnach entsprechend dem Eventualbegehren der Beklagten abzuweisen und die Empfehlung vom 9. Januar 2008 aufzuheben. Das Hauptbegehren der Beklagten um Rückweisung der Klageschrift an den Kläger ist dagegen abzuweisen, auf das Begehren der Beklagten, den Kläger zur Orientierung der Öffentlichkeit über die vorliegende Angelegenheit zu verpflichten, ist nicht einzutreten.

E. 15

Gemäss Art. 69 Abs. 1 BZP entscheidet das Gericht über die Prozesskosten von Amtes wegen nach den Art. 65, 66 und 68 des Bundesgerichtsgesetzes vom 17. Juni 2005 (BGG, SR 173.110).

E. 15.1

Dem in der Hauptsache unterliegenden Kläger, der in seinem amtlichen Wirkungskreis tätig geworden ist, werden gemäss Art. 66 Abs. 4 BGG keine Gerichtskosten auferlegt.

E. 15.2

Nach Art. 68 Abs. 2 BGG sind der obsiegenden Partei alle durch den Rechtsstreit verursachten notwendigen Kosten nach Massgabe des Tarifs des Bundesgerichts zu ersetzen. Nach Art. 1 des Reglements vom 31. März 2006 über die Parteientschädigung und die Entschädigung für die amtliche Vertretung im Verfahren vor dem Bundesgericht (nachfolgend Reglement über die Parteientschädigung, SR 173.110.210.3) gehören dazu die Anwaltskosten und allfällige weitere notwendige Kosten, die durch den Rechtsstreit verursacht worden sind. Die Anwaltskosten umfassen das Honorar und die notwendigen Auslagen des Anwalts oder der Anwältin (Art. 2 Abs. 1 Reglement über die Parteientschädigung). Hat der Streit kein Vermögensinteresse, so beträgt das Honorar, je nach Wichtigkeit und Schwierigkeit der Sache sowie nach Arbeitsaufwand, Fr. 600 - 18'000 (Art. 6 Reglement über die Parteientschädigung).

E. 15.3

Die Beklagte macht in ihrer Kostennote vom 12. Dezember 2008 eine Parteientschädigung über insgesamt Fr. 52'793.45, zusammengesetzt aus einem Anwaltshonorar von Fr. 52'097.10 bei einem Zeitaufwand von 249.75 Stunden und Spesen in der Höhe von Fr. 696.35, geltend. Der Sachverhalt sei kompliziert, sehr komplex und interdisziplinär und habe viele Fragen aufgeworfen. Es seien umfassende rechtsvergleichende Abklärungen nötig gewesen. Zudem hätten die redundanten und unstrukturierten Begründungen der Gegenpartei einen grossen Aufwand verursacht. Es sei ein Stundenansatz von Fr. 300.-- verrechnet und wo immer möglich ein Rechtspraktikant zum hälftigen Stundenansatz eingesetzt worden.

E. 15.4

Das Reglement über die Parteientschädigung sieht für Streitigkeiten ohne Vermögensinteresse ein Honorar von maximal Fr. 18'000.-- vor. Beansprucht eine Streitsache aussergewöhnlich viel Arbeit, können die Ansätze des Reglements überschritten werden (Art. 8 Abs. 1 Reglement über die Parteientschädigung). Die Beklagte ist mit ihrem Hauptbegehren auf Rückweisung der Klage zur Nachbesserung nicht durchgedrungen, wohl aber mit ihrem Eventualbegehren auf Abweisung der Klage. Unterlegen ist sie sodann mit ihrem Antrag auf Verpflichtung des Klägers zur Information der Öffentlichkeit, auf den nicht einzutreten ist. Da die Abweisung der Klage als Hauptpunkt des Prozesses anzusehen ist, kann die Beklagte als im Umfange von zwei Dritteln obsiegend angesehen werden. Hinsichtlich der Kostennote ist festzuhalten, dass diese zu einem erheblichen Teil Aufwendungen umfasst, die nicht das Klageverfahren betreffen und von vornherein nicht gestützt auf Art. 69 Abs. 1 BZP i.V.m. Art. 68 Abs. 2 BGG entschädigt werden können; beim Verfahren auf Erlass einer Empfehlung handelt es sich um ein Verwaltungsverfahren, für welches kein Anspruch auf Parteientschädigung besteht (vgl. BGE 132 II 47 E. 5.2). Bei grober Schätzung der auf das Verfahren vor dem Bundesverwaltungsgericht abfallenden Aufwendungen und in Würdigung aller Umstände - einerseits der Durchführung eines doppelten Schriftenwechsels, andererseits aber auch des Verzichts sowohl auf eine Vorbereitungs- als auch eine Hauptverhandlung nach Art. 35 und 66 ff. BZP sowie der teilweise weitschweifigen, unnötige Wiederholungen enthaltenden Parteieingaben der Beklagten - erscheinen Parteikosten in der Höhe von Fr. 25'500.-- als angemessen. Angesichts des bloss teilweisen Obsiegens sind diese um einen Drittel auf Fr. 17'000.-- zu kürzen. Unter dem Titel der Spesenentschädigung sind der Beklagten zusätzlich Fr. 240.-- auszurichten. Dies ergibt eine Parteientschädigung von insgesamt Fr. 17'240.-- (inkl. Mehrwertsteuer), welche ihr durch den Kläger zu entrichten ist.