

Aktuelle Entwicklungen im Datenschutzrecht

- Übersicht für den Anbieter von Telekommunikationsdiensten -

Mit diesem Whitepaper erhalten Sie einen Überblick über folgende aktuelle datenschutzrechtliche Themen:

- [Auskunftspflichten ggü. dem Rechteinhaber](#)
- [Vorratsdatenspeicherung](#)
- [Online-Durchsuchung](#)

1. Allgemeines

Dieses Whitepaper behandelt die aktuelle Rechtslage bei Gewährung von Auskunftsansprüchen im Spannungsfeld mit der datenschutzrechtlich zumindest problematischen Weitergabe von Kundendaten unter Berücksichtigung der Entscheidungen des BVerfG zur Vorratsdatenspeicherung und zur Onlinedurchsuchung. Gerade in den letzten Monaten gab es eine Reihe bedeutender Entwicklungen im Datenschutzrecht, die besonders für Unternehmer mit Tätigkeitsbereich im Internet von entscheidender Bedeutung sind. Im Folgenden soll ein Überblick über diese Neuerungen und daraus zu ziehende Konsequenzen gegeben werden.

2. Auskunftsansprüche / Drittauskunft

Am 1. 9. 2008 trat das Gesetz zur Durchsetzung der Rechte des geistigen Eigentums in Kraft.

Ein wichtiger Bestandteil dieses Gesetzes, beruhend auf der Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 19.04.2004 zur Durchsetzung der Rechte des geistigen Eigentums¹, war die Einführung/Neufassung der Auskunftsansprüche bezüglich der Gesetze zum Schutz der gewerblichen Schutzrechte bzw. der Gesetze zum Schutz des geistigen Eigentums².

Angelehnt an die europäische Vorgabe in der Durchsetzungs-RL sind die jeweiligen Vorschriften in den einzelnen Gesetzen jeweils identisch gefasst. Der Einfachheit halber wird hier nur auf den § 101 UrhG Bezug genommen, die Ausführungen sind jedoch auf die übrigen Schutzrechte übertragbar. Neu sind die jeweils in den Abs. 2 geregelten Ansprüche auf Drittauskunft gegen solche Personen, die keine Verletzer – auch keine Störer- sind. Hierzu später mehr.

Dieser Auskunftsanspruch ist sowohl für denjenigen, dessen Schutzrechte verletzt sind oder sein könnten von Bedeutung, als auch für diejenigen, der sich einem solchen Auskunftsanspruch ausgesetzt sieht. Da eine Auskunftspflicht immer auch eine Preisgabe von Daten Dritter bedeutet, ist gerade für all jene, die sich

¹ Abl L 195 vom 2.6.2006, S. 16ff (sog. Enforcement- oder Durchsetzungs-RL).

² § 140b PatentG, § 24b GebrauchsmusterG, § 19 MarkenG, § 101 UrhG, § 46 GeschmacksmusterG, § 37b SortenschutzG.



gemäß Abs. 2 der jeweiligen Auskunftsvorschriften einem Anspruch ausgesetzt sehen, der Konflikt zwischen Datenschutzvorschriften und einer Auskunftsverpflichtung problematisch. Darf man, oder muss man sogar Auskunft über vertrauliche Kundendaten geben, wenn dies von dem Schutzrechtinhaber verlangt wird?

Voraussetzung sowohl eines Auskunftsanspruches gegen den/die Verletzer als auch gegen Dritte gemäß § 101 Abs. 2 UrhG ist eine Verletzung in gewerblichem Ausmaß.

Hier hat die Rechtsprechung insbesondere im Bereich des Urheberrechtes bislang eine Reihe verschiedener Versuche unternommen, Kriterien für die Annahme eines solchen gewerblichen Ausmaßes zu entwickeln. Das Kriterium „gewerbliches Ausmaß“ ist nicht mit einem Handeln im geschäftlichen Verkehr gleichzusetzen. So kann auch ein privater Endverbraucher durchaus Rechtsverletzungen in gewerblichem Ausmaß begehen. Dies ist dann der Fall, wenn nach objektiven Umständen Anzahl bzw. Schwere der Rechtsverletzungen auf ein gewerbliches Ausmaß schließen lassen.

Die Schwere der Rechtsverletzung soll jedoch nicht an der Verletzung selbst gemessen werden, sondern zielt auf den verursachten Schaden ab.

Hier kann man am Beispiel Urheberrecht sagen, dass die Schwere einer Rechtsverletzung vom Marktanteil des verletzten Werkes ebenso abhängt wie von dem zeitlichen Verhältnis zur Veröffentlichung des Werkes. Je näher die Rechtsverletzung am Zeitpunkt der Veröffentlichung liegt, desto größer ist die wahrscheinliche Anzahl an unberechtigten Nutzungen und damit ist der Schaden umso größer.

Fehlt die Kontrolle über die Anzahl der Nutzungen spricht dies ebenfalls für ein gewerbliches Ausmaß, während die Bereitstellung für einen beschränkten Nutzerkreis, zu dessen Teilnehmern eine persönliche Beziehung besteht, dies eher ausschließt.

Liegt ein Handeln im gewerblichen Ausmaß vor, so ist gegenüber dem Verletzer (inkl. Störer) ein Auskunftsanspruch gegeben.

Gegenüber Dritten muss jeweils noch eine offensichtliche Rechtsverletzung gegeben sein, damit eine gesetzliche Verpflichtung zur Auskunft angenommen werden kann.

Da eine solche offensichtliche Rechtsverletzung die in Anspruch genommenen Unternehmen jeweils schwerlich im Einzelfall feststellen können, käme man hier regelmäßig in Konflikt mit dem Datenschutz gegenüber den eigenen Kunden.

Hier steht jedoch z.B. § 101 Abs. 6 UrhG mit einer Haftungserleichterung bereit.

Zumindest für den Fall, dass eine wahre Auskunft erteilt wurde, besteht eine Haftung gegenüber den Kunden nur dann, wenn Kenntnis bezüglich der fehlenden Verpflichtung zur Auskunftserteilung bestand. Geht somit z.B. ein Provider von einer offensichtlichen Rechtsverletzung aus, haftet er dann auch nicht gegenüber Dritten, wenn der Anspruch entgegen dieser Annahme nicht bestand.

Schließlich kann sich derjenige, welcher ohne selbst Rechtsverletzer zu sein zu einer Auskunft verpflichtet wurde, die Kosten der Auskunft vom Verletzten erstattet verlangen (z.B. § 101 Abs. 2 S. 3 UrhG).

Problem: Ermittlung der IP-Adresse

Personenbezogene Daten dürfen laut § 4 Abs. 2 S. 1 BDSG beim Betroffenen nur mit dessen Kenntnis

erhoben werden. Allein der Umstand, dass die IP-Adresse automatisch bei Aufbau einer Internetverbindung bekannt gegeben wird, genügt hierfür nicht. Vielmehr muss der Betroffene die Datenerhebung bewusst dulden³.

Um den Nutzer eines Internetangebotes identifizieren zu können, bedarf es im Regelfall der Ermittlung der IP-Adresse.

Die meisten (privaten) Nutzer verwenden hier keine statischen, sondern lediglich von Internetsitzung zu Internetsitzung neu vergebene sog. dynamische IP-Adressen.

Ob es sich bei einer IP-Adresse um ein personenbezogenes Datum handelt, ist in der Rechtsprechung bislang umstritten⁴. Hier bleibt die Entwicklung der ober- und höchstgerichtlichen Rechtsprechung abzuwarten. Vertritt man jedoch die Ansicht, dass es sich bei einer dynamischen IP-Adresse um ein personenbezogenes Datum handelt, kann eine auf § 101 UrhG gestützte Auskunft sogar einem Beweisverwertungsverbot unterliegen.

Werden Verkehrsdaten übermittelt, stellt dies einen Eingriff in Art. 10 GG (Fernmeldegeheimnis) dar. Ein solches Vorgehen bedarf deshalb eines richterlichen Beschlusses. Insofern ist auch nach der geltenden Gesetzeslage eine effektive Durchsetzung der Rechte der Anspruchsinhaber keineswegs so eindeutig gewährleistet, wie es zunächst den Anschein macht.

3. Vorratsdatenspeicherung

Rechtslage nach Beschluss des BVerfG vom 11. März 2008

Am 1. Januar 2008 trat das Gesetz zur Neuregelung der TK-Überwachung und anderer verdeckter Ermittlungsmaßnahmen in Kraft und damit auch der § 113a TKG, der Anbieter von Telekommunikationsdiensten zur Vorratsdatenspeicherung verpflichtet.

Über die gegen diese Verpflichtung eingelegte Verfassungsbeschwerde wurde zwar noch nicht entschieden, wohl ist jedoch am 11. März 2008 eine einstweilige Anordnung des BVerfG ergangen.

Hierin hat das BVerfG zunächst nur entschieden, die Nutzung der im Rahmen der Vorratsdatenspeicherung gewonnenen Daten, zumindest bis zur endgültigen Entscheidung über die Verfassungsbeschwerde, nur auf bestimmte Anlässe der Strafverfolgung zu beschränken. Der Datenabruf soll –zumindest vorübergehend– deshalb nur eingeschränkt möglich sein, während die Speicherung im Vorfeld dieses Abrufes zunächst weiterhin zu erfolgen hat.

Im Falle der Datenerhebung konkretisieren sich die Nachteile für den Einzelnen durch die Vorratsdatenspeicherung dann erst bei Abruf dieser Daten. Deshalb sei der Vollzug der zur Vorratsdatenspeicherung verpflichtenden Vorschrift des § 113a TKG nicht im Wege einer einstweiligen Verfügung auszusetzen. Die §§ 100g Abs. 1, Abs. 2 Satz 1 iVm § 100b Abs. 1 und 2 StPO geben eine Rechtsgrundlage für ein Abrufersuchen an den TK-Dienstleister im Falle von Straftaten von erheblicher Bedeutung. Allerdings stünden bereits nach Ansicht des

³ Siehe hierzu u.a. Stefan Maaßen, „Urheberrechtlicher Auskunftsanspruch und Vorratsdatenspeicherung“, in MMR 2009, S. 511, 513.

⁴ Für eine Übersicht siehe Maaßen, aaO. S. 513.

BVerfG die europarechtlichen Vorgaben einer einstweiligen Anordnung zur Aussetzung der Speicherpflicht der Vorratsdaten im Wege.

Beschluss des VG Berlin

- Entbindung von der Pflicht Technik zur Vorratsdatenspeicherung bereit zu halten -

Nach dem Beschluss des BVerfG vom 11. März 2008 ist der Telekommunikationsanbieter somit grundsätzlich verpflichtet, weiterhin eine Vorratsdatenspeicherung vorzunehmen. Lediglich die Weiterleitung der gespeicherten Daten solle auf Fälle von Straftaten von erheblicher Bedeutung beschränkt werden.

Deshalb sind Anbieter von Telekommunikationsleistungen verpflichtet, mit großem finanziellen Aufwand die technische Möglichkeit der geforderten Vorratsdatenspeicherung zu gewährleisten. Bei Erfolg der eingelegten Verfassungsbeschwerde wären diese Investitionen jedoch nutzlos gewesen. Deshalb hat das VG Berlin mit Rücksicht auf die möglichen finanziellen Folgen die Speicherungspflicht vorläufig ausgesetzt⁵. Zumindest auf eigene Kosten ist nach diesem Beschluss kein Anbieter von Telekommunikationsdienstleistungen verpflichtet, Technik zur Vorratsdatenspeicherung bereit zu halten bis das BVerfG endgültig über die Verfassungsbeschwerde entschieden hat.

4. Onlinedurchsuchung

In einer Entscheidung des BVerfG wurde das nordrhein-westfälische Verfassungsschutzgesetz, das eine Befugnis zur Onlinedurchsuchung vorgesehen hatte, für verfassungswidrig erklärt.

Eine Onlinedurchsuchung ist nach Ansicht des BVerfG nur dann verhältnismäßig, wenn Anhaltspunkte einer konkreten Gefahr für ein überwiegend wichtiges Rechtsgut bestehen. Darunter fallen Leib, Leben und Freiheit einer Person sowie Güter der Allgemeinheit deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Unterhalb der genannten Rechtsgüter greife eine Onlinedurchsuchung unverhältnismäßig in die Rechte des Durchsuchten ein. Hier sah das BVerfG das in dieser Entscheidung entwickelte „Computergrundrecht“ auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme verletzt.

Da staatliche Eingriffe in diesen Vertrauensbereich besonders schwer wiegen, soll nach Ansicht des BVerfG für einen solchen Eingriff eine besondere gesetzliche Legitimation vorliegen. Neben der vorherigen Entscheidung über den Zugriff einer unabhängigen Instanz müsse zudem gewährleistet sein, dass die Betroffenen im Nachhinein von dem Eingriff benachrichtigt werden.



⁵ VG Berlin, Beschluss vom 17. Oktober 2008 - VG 27 A 232.08

Weitere Informationen hierzu erteilt Ihnen gerne:

Herr Rechtsanwalt Sascha Faber, LL.M. (Medienrecht):

faber@volke2-0.de

Fon: 02306/75684-0

Fax: 02306/75684-11

Der Autor, Herr Rechtsanwalt Sascha Faber LL.M. (Medienrecht) ist, wie alle Anwälte der Kanzlei Volke2.0, ausschließlich auf den Gewerblichen Rechtsschutz (Wettbewerbs-, Marken-, Gebrauchs-, Geschmacksmuster- und Patentrecht) im Internet und das IT-Recht spezialisiert. Das Team von Volke2.0 steht Ihnen gerne auch für weitere Fragen rund um diese Rechtsgebiete zur Verfügung.

Bitte beachten Sie, dass dieses White Paper lediglich zur Information und Orientierung in dem entsprechenden Bereich des Rechts dient. Das Dokument kann nur als Hilfestellung verwendet werden. Im konkreten Einzelfall sollte eine rechtliche Beratung durch einen Rechtsanwalt in Anspruch genommen werden. Dieses White Paper ist nicht dazu gedacht, eine anwaltliche Beratung zu ersetzen. Eine Haftung kann daher nicht übernommen werden.