Thomas Hoeren, Jonas Völkel

Informationsabfrage über Domainverantwortliche nach der DS-GVO

Zur datenschutzrechtlichen Zulässigkeit einer Abfrage von Informationen über Domainverantwortliche nach der DS-GVO

Nach der Datenschutz-Grundverordnung (DS-GVO) tobt der Streit, ob und inwieweit die im Internet frei zugänglichen Daten des Domaininhabers und anderer Personen weiterhin der Öffentlichkeit zugänglich gemacht werden dürfen. Der vorliegende Beitrag überprüft die Zulässigkeit dieser Tradition im Domainrecht und weist auf erhebliche Schwächen und deren Lösung hin. Die DS-GVO sieht wie das deutsche Datenschutzrecht ein grundsätzliches Verbot der Datenverarbeitung mit Erlaubnisvorbehalt vor. Jedoch sind gerade die Erlaubnistatbestände an einigen Stellen enger als im deutschen Recht. Das entwickelt sich aktuell zum Verhängnis der Anbieter von Diensten zur Abfrage von Daten über Domaininhaber.

1 Problemstellung

Über „whois" und ähnliche Dienste können bisher von jedem beliebigen Nutzer persönliche Daten über Domainbetreiber abgerufen werden. Dafür werden Kontaktdaten von Domaininhaber, AdminC, TechC oder BillingC erhoben, gespeichert und im Rahmen der Abfragen veröffentlicht. Die betroffenen Domainverwalter haben zurzeit keine Möglichkeit, gegen diese Art der Verarbeitung ihrer Daten vorzugehen.[1] Nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) ist es fraglich, ob und unter welchen Voraussetzungen diese Praxis datenschutzrechtlich zulässig ist. Die Debatte wird momentan mit so viel Nachdruck geführt, dass sogar die ansonsten für europäische Belange wenig kompromissbereite ICANN mit übergangsweisem Einlenken reagierte.[2]

Name und Kontaktadresse des Domaininhabers, AdminC, TechC und BillingC sind personenbezogene Daten, deren Verarbeitung im Geltungsbereich der Datenschutz-Grundverordnung eines gesetzlichen Erlaubnistatbestandes oder einer Einwilligung bedarf. Art. 6 Abs. 1 gestattet demgegenüber die Verarbeitung ohne Einwilligung, wenn sie für die Erfüllung eines Vertrages (lit. a) oder zur Wahrung berechtigter Interessen erforderlich ist, ohne dass Grundrechte oder Grundfreiheiten des Betroffenen überwiegen (lit. f).

Die momentane Praxis geht bisher ohne Einholung einer datenschutzrechtlichen Einwilligung vor. Schon aus Praktikabilitätsgründen werden die Anbieter wohl auch für die zukünftige Gestaltung der Abfrage eine gesetzlich legitimierte Lösung bevorzugen. Daher soll im Folgenden zunächst Augenmerk auf die Erlaubnistatbestände gelegt werden (2-3), bevor dann auf die Bedingungen einer Einwilligungslösung näher eingegangen wird (4).

Professor Dr. Thomas Hoeren

Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Universität Münster

E-Mail: hoeren@uni-muenster.de

Jonas Völkel

Wissenschaftlicher Mitarbeiter am ITM, Universität Münster

E-Mail: jonas.voelkel@uni-muenster.de

1 Vgl. Hager/Gsell/Krüger/Lorenz/Reymann/*Koch*, beck-online Grosskommentar, BGB § 12, Rn. 122.

2 ZD-Aktuell 2017, 05848.

2 Erforderlich zur Erfüllung eines Vertrags

Um von der ersten Alternative des Erlaubnistatbestands zu profitieren, müssten alle Verarbeitungshandlungen zur Erfüllung eines Vertrags zwischen dem Abfrageanbieter und den Domainbetreibern erforderlich sein. In der Regel ist es ein Domain Name Registrar, der eine Vertragsbeziehung zum Endkunden eingeht, der eine Domain betreiben will.[3] Zur Abwicklung dieses Geschäfts ist die Erhebung und Speicherung des Namens des Vertragspartners, seiner Anschrift und technischer Informationen erforderlich.

Nicht erforderlich ist es allerdings, dass die Registry neben dem Registrar ebenfalls diese Daten vorhält. Sie ist üblicherweise nicht in die Abwicklung des Vertrags zwischen Registrar und Endkunden eingebunden und benötigt keine Daten von Domaininhabern zur Durchführung ihrer Verträge mit dem Registrar. In der momentanen Praxis ist es aber die Registry-Stelle, die als Anbieter der Datenabfragen auftritt. Zwar besagt etwa Nr. VII 1 der DENIC-Domainrichtlinien,[4] dass der Domaininhaber Vertragspartner der DENIC sei; diese Regelung in Form von AGB kann aber nur inter partes gelten und hat somit nur dann Wirkung, wenn tatsächlich ein Vertrag mit der DENIC direkt geschlossen wird.

Ferner ist es auch für den Registrar nicht ohne weiteres erforderlich, Daten von AdminC, TechC und BillingC zu erheben und zu speichern. Die Registrierung der Domain für den Domaininhaber und die Abrechnung mit ihm erfordern keine Daten von weiteren Verwaltungseinheiten der Domain auf Endnutzerebene.

Schon gar nicht erfordert es die Vertragserfüllung, die Daten öffentlich zum Abruf bereitzustellen.

3 Wahrung berechtigter Interessen

Die Verarbeitung der Daten von Domaininhaber, AdminC, TechC und BillingC durch die Registry und deren Veröffentlichung ist möglicherweise erforderlich, um berechtigte Interessen der Registry oder der Öffentlichkeit im Sinne des Art. 6 Abs. 1 lit. f DS-GVO zu wahren.

Die Veröffentlichung der Daten wurde bisher damit begründet, den Kontakt zum Domaininhaber bei technischen Problemen und eventuellen Rechtsverletzungen zu kontaktieren. Dazu schrieb der hessische Landesdatenschutzbeauftragte im Datenschutzbericht aus dem Jahr 2000, dass die „Veröffentlichung von Name und Anschrift der Domain-Inhaber bei der DENIC eG [...] erforderlich ist, um den zuverlässigen Betrieb des Netzes in Deutschland sicherzustellen"; die Veröffentlichung trage „erheblich zur Förderung der Rechtssicherheit i. S. d. Verbraucherschutzes im Internet bei".[5] In der Tat ist das Interesse der Öffentlichkeit daran, den technisch und rechtlich Verantwortlichen Betreiber einer Domain zu kennen, legitim. Wenn Internetseiten in voller Anonymität betrieben würden, dann wäre eine Rechteverfolgung nicht möglich. Auch Verbraucherinteressen anzuführen, ist gerechtfertigt.[6] Betrügerische Internetauftritte könnten in voller Anonymität nicht von Behörden oder Verbraucherschutzorganisationen bekämpft werden. Fraglich ist allerdings, ob der „zuverlässige Betrieb des Netzes in Deutschland" private Daten der Domaininhaber erfordert. Technische Probleme einzelner Domains sind zunächst das alleinige Problem des Inhabers. Zwar besteht unter Umständen ein Interesse an der Nutzung, aber es ist allein die Entscheidung des Domaininhabers, Dienste bereitzustellen oder nicht. Nur wenn bestimmte Domains und ihre Dienste Schlüsselrollen im Netz einnehmen, ist der zuverlässige Betrieb des Netzes über die einzelne Domain hinaus gefährdet. Dass in der dezentralen Struktur des Internet verschiedene Seiten stark vernetzt sind, ändert daran nichts, solange der Großteil technisch zuverlässig läuft.

Allerdings muss die Abwägung der gegenseitigen Interessen nach der Datenschutz-Grundverordnug neu bewertet werden, denn Datensparsamkeit und Privacy by Default gehören zu ihren ausdrücklich erklärten Zielen. Die pauschale Bereitstellung persönlicher Daten für die Öffentlichkeit steht in klarem Konflikt zu diesen Zielen. Im Grunde scheitert schon hier die Veröffentlichung der persönlichen Daten aller anderen Domainverwaltungseinheiten neben dem Domaininhaber (wie AdminC, TechC und BillingC). Die Kenntnis eines einzelnen Verantwortlichen genügt für die Wahrung der Interessen.

Im Rahmen des Art. 6 Abs. 1 lit. f DS-GVO sind zudem Grundrechte- und Freiheiten des Betroffenen zu berücksichtigen. Evidenterweise ist das Recht auf Schutz personenbezogener Daten aus Art. 8 EU-Grundrechtecharta betroffen, ebenso das Recht auf Achtung des Privat- und Familienlebens aus Art. 8 EMRK[7] und das Grundrecht auf informationelle Selbstbestimmung aus dem deutschen Grundgesetz.[8] Diese Grundrechte gelten direkt zwar nur gegenüber dem Staat, über die Einbeziehung in den Wortlaut des Art. 6 Abs. 1 lit. f DS-GVO entfalten sie hier aber mittelbare Drittwirkung und sind im Rahmen der Interessenabwägung auch zulasten Privater wirksam.[9] Daneben hat die Veröffentlichung solcher Daten aber noch andere grundrechtsrelevante Auswirkungen: Wird etwa eine Homepage mit kontroversem politischen Inhalt betrieben, so hat der Inhaber unter Umständen ein Interesse daran, dass die breite Öffentlichkeit nicht uneingeschränkt Einsicht darin hat, wer hinter den Aussagen steht. Die Meinungsfreiheit schützt nämlich auch das Interesse, eine politische Meinung in demokratischen Auseinandersetzungen anonym zu äußern. Es soll verhindert werden, dass Meinungen aus Angst vor Repressalien oder anderen negativen Auswirkungen nicht geäußert werden.[10] Das Argument, es bestehe grundsätzlich kein Geheimhaltungsinteresse, weil die Daten sowieso im Rahmen der Impressumspflicht öffentlich gemacht werden müssen,[11] überzeugt nicht: Das Impressum dient anderen Zwecken und umfasst nicht zwingend die gleichen Daten. Zum einen ist der Dienstanbieter von einem Internetauftritt, der im Impressum auftaucht, oft nicht die gleiche Person wie der Domaininhaber und zum anderen gilt die Impressumspflicht nur für gewerb-

3 Vgl. https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en (letzter Zugriff: 12.1.2018).

4 Abrufbar unter: https://www.denic.de/domainrichtlinien/ (letzter Zugriff: 12.1.2018).

5 *Hessischer Landtag*, Datenschutzbericht 2000, Drucksache 15/1539, S. 23.

6 Vgl. *Ermert*, Datenschutz: Eco-Verband springt für ICAN in die Bresche, abrufbar unter: https://www.heise.de/newsticker/meldung/Datenschutz-Eco-Verband-springt-fuer-ICANN-in-die-Bresche-3877085.html (letzter Zugriff 12.1.2018).

7 *Meyer-Ladewig/Nettesheim*/von Raumer, Europäische Menschenrechtskonvention, Art. 8 Rn. 32.

8 *Jarass*/Pieroth, Grundgesetz Art. 2 Rn. 39; Sachs/*Murswiek/Rixen*, Grundgesetz Art. 2 Rn. 72 f.

9 *EuGH*, Urteil vom 13.05.2014 – C-131/12; Ehmann/Selmayr/Heberlein, Datenschutzgrundverordnung Art. 6 Rn. 24; Maunz/Düring/*Di Fabio*, Grundgesetz Art. 2 Rn. 191.

10 *EGMR*, NJW 2015, 2863 (2864 ff.).

11 *Hessischer Landtag*, Datenschutzbericht 2000, Drucksache 15/1539, S. 23.

liche Websites. Außerdem spräche das Argument eher gegen ein Verarbeitungsinteresse als gegen ein Geheimhaltungsinteresse: Da die Daten ohnehin im Impressum stehen – und der Impressumspflichtige den Inhalten meist sogar näher steht als der Domaininhaber – müssen nicht zusätzliche Daten an anderer Stelle einsehbar sein.

Die Interessen von Öffentlichkeit, also der Nutzer, und Inhaber eventuell verletzter Rechte, müssen gegen die der Domaininhaber abgewogen werden. Dabei ist zu berücksichtigen, ob dem Verarbeitungsinteresse auch mit einem milderen, respektive datensparsameren Mittel gleich effektiv Rechnung getragen werden kann. Hier sind verschiedene Möglichkeiten denkbar, dass Rechteinhaber oder sonstige Stellen, die ein berechtigtes Interesse an der Kenntnis der Daten haben, gezielt Auskunft über einzelne Daten bekommen.

Davon werden insbesondere zwei Modelle diskutiert: Eine Möglichkeit ist, eine geschlossene whois-Alternative anzubieten, auf die nur privilegierte Gruppen wie bestimmte Behörden Zugriff haben. Die andere ist, generell nur Einzelanfragen zuzulassen, bei denen ein berechtigtes Interesse im Einzelfall konkret nachgewiesen werden muss.

3.1 Zugriff privilegierter Nutzergruppen

Das erste Modell ist ein Kompromiss, der Datenschutzinteressen offensichtlich stärker beeinträchtigt als das zweite. Der Abruf ist schneller und erlaubt auch automatisiertes und systematisches Durchsuchen sowie Profilbildung. Das kommt zurzeit etwa bei Rasterfahndungen nach Rechtsverstößen im Domainbereich – auch durch Privatleute[12] – zum Einsatz.[13] Datenschützern ist gerade Profilbildung und Rasterfahndung ein Dorn im Auge.[14] Allerdings gibt es auch schützenswerte Interessen, die allein mit solchen Recherchemitteln verwirklicht werden können: Zum Beispiel ist im Beschwerdeverfahren bei der ICANN Bösgläubigkeit bei der Domainregistrierung dadurch nachweisbar, dass der Inhaber mehrere Domains registriert, die einer geschützten Marke ähnlich sind und sich daraus ein klares Verhaltensmuster ergibt („pattern of such conduct").[15] Für den Fall, dass die vorliegende Domain der eigenen Marke zwar ähnlich ist, aber noch keine klare Verletzung vorliegt, muss der Beschwerdeführer nachweisen, dass aus einer Mehrzahl von Domains des Beschwerdegegners ein solches Verhaltensmuster folgt.[16] Dazu ist es erforderlich, zu ermitteln, welche anderen Domainnamen der gleiche Inhaber noch registriert hat. Allerdings ist es äußerst fragwürdig, ob die problematischere Beweisführung in Einzelfällen einen generellen und flächendeckenden Eingriff in die Privatsphäre aller Domainverwalter rechtfertigt. Wenn privilegierte Stellen einen Zugriff haben, können darüber auch einem Beschwerdeführer Möglichkeiten gegeben werden, seine Interessen geltend zu machen. Vergleichbar ist das mit der Auskunft über Verbindungsdaten einer IP-Adresse bei festgestellten Rechtsverstößen im Internet.

3.2. Einzelanfragen

Das zweite Modell bietet den effektivsten Datenschutz, der bei Wahrung der Öffentlichkeitsinteressen möglich ist. Denn durch Einzelanfragen ist es einerseits überhaupt möglich, an die Daten zu gelangen; andererseits kann der Zugriff durch Prüfungsverfahren so restriktiv wie möglich gehalten werden. Rasterfahndungen sind damit erheblich eingeschränkt. Dennoch gibt es Lösungen für Probleme, wie sie das oben beschriebene Beschwerdeverfahren bei bösgläubiger Domainregistrierung stellt: Für solche Fälle liegt schon durch die Ähnlichkeit des Domainnamens mit der Marke ein berechtigtes Interesse nahe, so dass eine Abfrage gerechtfertigt wäre. Ein solches Interesse kann auch ein umfangreiches Auskunftsgesuch rechtfertigen, solange es um einen Einzelfall mit konkret nachgewiesenem Interesse handelt.

Bei der Entscheidung zwischen den beiden Modellen ist die konkrete Umsetzung Dreh- und Angelpunkt eines angemessenen Interessenausgleichs. So ist zum Beispiel zu entscheiden, bei welcher Stelle Daten gespeichert und abgerufen werden. Zunächst liegen die Daten beim Registrar. Welcher Registrar hinter einer Domain steckt, ist von außen nicht ohne weiteres erkennbar. Auch eine automatisierte Anfrage müsste zunächst in Einzelabfragen ermitteln, wo die Daten abgerufen werden können. Im Endeffekt kann den Öffentlichkeitsinteressen nur effektiv Rechnung getragen werden, wenn eine wie auch immer gestaltete Abfrage zentral bei der Registry gestellt werden kann. Dann müssten die Daten entweder auch bei der Registry zentral gespeichert werden, oder aber der Abruf sieht eine Weiterleitung zu den Datenbanken der Registrare vor. Das gleiche gilt für nichtautomatisierte Einzelanfragen. Auch dabei müsste entweder aus einer zentralisierten Datenbank geschöpft oder die Anfrage zweistufig bearbeitet werden: Der Öffentlichkeit ist zunächst über die Top Level Domain nur die Registry bekannt. Daher muss im ersten Schritt bei ihr der Registrar abgefragt werden, bei dem im zweiten Schritt die Einzelauskunft eingeholt werden kann. Dabei sollte es datenschutzrechtlich nicht problematisch sein, die Abfrage auf der ersten Stufe automatisiert und offen zugänglich zu gestalten. Durch die Verknüpfung von Domain und Registrar fallen in der Regel keine personenbezogenen Daten an.

Werden Daten zusätzlich bei einer Stelle gespeichert, die nicht Vertragspartner des Domaininhabers ist, so fallen nicht nur mehr Daten an; die Daten liegen auch weiter vom Kontrollbereich des Betroffenen entfernt und die Missbrauchsgefahr ist bei zentralisierten Datenbanken höher. Das widerspricht den in der Datenschutz-Grundverordnung verankerten Grundsätzen von Datensparsamkeit und Privacy by Default. Eine dezentrale Abfrage hingegen birgt praktische Probleme, die einer effizienten Interessendurchsetzung entgegenstehen können. Das mildeste erforderliche Mittel im Sinne des Art. 6 Abs. 1 lit. f DS-GVO ist wohl in einer praktisch funktionellen Umsetzung einer dezentralen Abfrage zu suchen. Die Interessenlage ist vergleichbar mit Auskünften über Anschlussinhaber im Telefonnetz: Seit Telefonbücher nicht mehr vollständig öffentlich zugänglich sind, steht der Rufnummerninhaber grundsätzlich pseudonym hinter seiner

12 *Cirosec*, Private Rasterfahndung – Profiling und Geolocation mittels Open-Source-Tool und GSM-Daten, abrufbar unter: https://www.cirosec.de/fileadmin/pdf/Berichterstattung.../searchsecurity.de_17.03.pdf (letzter Zugriff: 12.1.2018).

13 Vgl. *Ermert*, eco-Konzept für Domain-Daten – Das offene Whois vor dem Aus, abrufbar unter: https://www.heise.de/newsticker/meldung/eco-Konzept-fuer-Domain-Daten-Das-offene-Whois-vor-dem-Aus-3916669.html (letzter Zugriff: 12.1.2018).

14 BVerfG, Beschl. v. 4.4.2006 – 1 BvR 518/02; *Gola*, Datenschutz-Grundverordnung, Einleitung Rn. 37; Paal/Pauly/*Martini*, Datenschutz-Grundverordnung, Art. 22 Rn. 21 ff.; Sydow/*Ziebarth*, Europäische Datenschutzgrundverordnung, DSGVO Art. 4 Rn. 92.

15 Uniform Domain-Name Dispute-Resolution Policy (UDRP), Nr. 4 lit. b ii.

16 *WIPO Arbitration and Mediation Centre*, Entscheidung des Beschwerdepanels Deutsche Telekom AG v. Andreas Kusch – Verfahren Nr. D2008-0768, abrufbar unter: http://www.wipo.int/amc/en/domains/decisions/html/2008/d2008-0768.html (letzter Zugriff: 12.1.2018).

Nummer – vergleichbar mit dem Domaininhaber und der Domain. Über die Auskunftsverfahren unter den gesetzlichen Maßgaben der §§ 111-113 TKG haben jedoch öffentliche Stellen die Möglichkeit, Daten über Anschlussinhaber gezielt abzufragen.[17] Private Stellen sind darauf verwiesen, Auskünfte über ein freiwilliges Teilnehmerverzeichnis einzuholen (§§ 104 f. TKG) oder im Falle eines berechtigen Interesses ein Auskunftsersuchen bei der BNetzA nach § 66i TKG zu stellen. § 66i Abs. 3 TKG ist ein Beispiel für eine zweistufige Auskunft.[18] Anders als bei der bloßen Verknüpfung einer Telefonnummer mit Namen und Kontaktdaten der Anschlussinhaber sind mit der Domain allerdings direkte inhaltliche Informationen verbunden. Zwar muss der Domaininhaber nicht zwingend Betreiber einer Website sein; es ist jedoch offensichtlich, dass er in Verbindung mit dem Betreiber steht und somit zwangsläufig eine Verbindung zu den Inhalten gezogen wird. Das betrifft sein Recht auf informationelle Selbstbestimmung stärker als nur Informationen über Umstände der Kommunikation.[19] Außerdem kommt hier der oben beschriebene Effekt auf die Meinungsfreiheit zum Tragen. Eine bloße Ausnahme von einer generellen Veröffentlichung für Härtefälle – etwa Seiten mit politischem Inhalt – genügt den Anforderungen nicht: Allein die Entscheidung darüber würde Eingriffe in Grundrechte und -freiheiten erfordern und wäre kein Privacy by Default.

3.3 Fazit

Die Weitergabe von Daten des Domaininhabers lässt sich zugunsten berechtigter Interessen der Allgemeinheit rechtfertigen, was eine Datenverarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO möglich macht. Allerdings hängt die Erlaubnis der Verarbeitung stark von der tatsächlichen Umsetzung der Abfragelösung ab. Den Datenschutzinteressen des Domaininhabers muss effektiv Rechnung getragen werden. Die offene Abfrage, wie sie im Moment der Praxis entspricht, ist durch gesetzliche Erlaubnistatbestände der Datenschut-Grundverordnung nicht zu rechtfertigen.

4 Wie müsste eine Einwilligung gestaltet sein?

Man könnte daher darüber nachgedenken, über die Einwilligung des Betroffenen umfangreiche Datenverarbeitung möglich zu machen. Die Einwilligung des Betroffenen bietet neben der gesetzlichen Erlaubnis eine zweite Möglichkeit der legalen Datenverarbeitung. Eine Einwilligungslösung wäre über Domainverträge einfach umzusetzen. Dabei müssten die gesetzlichen Vorgaben zur datenschutzrechtlichen Einwilligung aus Art. 7 DS-GVO eingehalten werden.

Allerdings ist es fraglich, ob im Domainvertrag die Domainregistrierung von der Einwilligung abhängig gemacht oder eine Einwilligungsmöglichkeit nur vom Vertragsschluss getrennt wirksam werden kann. Im Rahmen der Frage, ob eine Einwilligung freiwillig abgegeben wurde, spielt nämlich das sogenannte Kopplungsverbot nach Art. 7 Abs. 4 DS-GVO eine wesentliche Rolle. Es erschwert die Bedingungen für die Freiwilligkeit einer datenschutzrechtlichen Einwilligung, wenn vertragliche Leistungen von der Abgabe der Einwilligung abhängig gemacht werden, ohne dass die Datenverarbeitung für die Erbringung dieser Leistungen notwendig wäre.[20] Da die Weiterleitung der Daten an andere Stellen als dem Registrar für Zwecke des Vertrags nicht erforderlich ist (s.o.), muss nach dem Gesetz dem Umstand der Kopplung des Vertrags an die Einwilligung „in größtmöglichem Umfang Rechnung getragen werden". Das bedeutet nicht, dass eine Kopplung per se ausgeschlossen ist, aber die Freiwilligkeit ist so weit wie möglich sicherzustellen.[21] Es spricht vieles dafür, dass die Einwilligung dann nicht freiwillig ist, wenn der Betroffene keine Möglichkeit hat, die vertragliche Leistung an anderer Stelle ohne die entsprechende Einwilligung zu bekommen. Das ist etwa dann der Fall, wenn der Verantwortliche besondere Marktmacht oder eine Monopolstellung innehat.[22] Eine effektive Gestaltung der whois-Anfrage müsste bei der Registry zentralisiert werden und diese hat hinsichtlich der Domainvergabe über lizensierte Registrare eine Monopolstellung. Zum gleichen Ergebnis führt es, wenn alle Anbieter nach Absprache eine solche Einwilligung fordern, um ein vollständiges Abfragesystem zu etablieren. Die genauen Voraussetzungen der noch jungen Datenschutz-Grundverordnung-Vorschriften sind hier noch lange nicht geklärt, so dass eine reine Einwilligungslösung bei der whois-Anfrage nur schwache Rechtssicherheit bergen würde.

Möglich ist jedoch eine nicht zwingende, das heißt vom Domainvertrag entkoppelte Einwilligung in ein öffentliches Register, das als Lösung zusätzlich zur Einzelabfrage angeboten wird. Auch hier ist der Vergleich mit Anschlussinhaberdaten von Telefonnetzen anschaulich: Seit der Privatisierung ist für Netzinhaber ein Zwang zum Eintrag in ein Telefonregister undenkbar.[23]

5 Ergebnis

Ein öffentliches whois ist gegen den Willen der Domaininhaber nach der Datenschutz-Grundverordnung nicht (mehr) möglich. Datenschutzrechtlich ist es zwar erlaubt, Auskunftssysteme einzurichten; diese müssen aber entweder von der freiwilligen Einwilligung der Betroffenen gedeckt oder aber so gestaltet sein, dass sie dessen Datenschutzinteressen in angemessener Weise Rechnung tragen. Das ist etwa dann der Fall, wenn Anfragen nur im Einzelfall bei konkret nachgewiesenem berechtigen Interesse beantwortet werden. Eine solche Lösung kann ohne Probleme zum Vorteil der Nutzer dadurch unterstützt werden, dass ein freiwilliges Register mit öffentlicher Abfrage bereitgestellt wird. Mit hoher Wahrscheinlichkeit darf die Domainregistrierung nicht grundsätzlich von der Einwilligung dazu, dass Daten in einem solchen Register erscheinen, abhängig gemacht werden.

17 *Graf*, BeckOK StPO mit RiStBV und MiStra, TKG § 111 Rn. 1-3; Geppert/Schütz/*Eckhardt*,, Beck'scher TKG-Kommentar, TKG § 111 Rn. 1f.

18 Geppert/Schütz/*Ditscheid/Rudloff*, Beck'scher TKG-Kommentar, TKG § 66i Rn. 2.

19 *Weichert*, Datenschutz im Auto – Teil 1, SVR 2014, 201 (203); vgl. auch Forgó/Helfrich/Schneider/*Hawellek*, Betrieblicher Datenschutz, Rn. 104 f.; Möstl/Schwabenbauer/Bär, Polizei und Sicherheitsrecht Bayern, PAG Art. 34a Rn. 27 f.

20 Gola/*Schulz*, Datenschutz-Grundverordnung, Art. 7 Rn. 22.

21 Wolff/Brink/*Stemmer*, BeckOK Datenschutzrecht, DS-GVO Art. 7 Rn. 42.

22 Wolff/Brink/*Stemmer*, BeckOK Datenschutzrecht, DS-GVO Art. 7 Rn. 43.

23 *Hoeren*, Das Konzerntelefonverzeichnis – ein datenschutzrechtlicher Sündenpfuhl? – Problemstellung und rechtliche Grenzen, ZD 2014, 441 f.