

# JONES DAY

RECHTSANWÄLTE • ATTORNEYS AT LAW • PATENTANWÄLTE  
NEUER STAHLHOF • BREITE STRASSE 69 • D-40213 DÜSSELDORF  
TELEFON: (49) 211 5 40 65 500 • TELEFAX: (49) 211 5 40 65 501

25. Mai 2018

**Vorab per Telefax (ohne Anlagen): 0228 702-1600**

**Per Kurier**

Landgericht Bonn

Kammer für Zivilsachen mit Internetbezug

Wilhelmstraße 21

53111 Bonn

DR. JAKOB GUHN

Büro Düsseldorf

Sekretariat: Frau Salowski

Tel. 0211-5406-5532

Unser Zeichen: 530198-610043 JG

## Antrag auf Erlass einer einstweiligen Verfügung

der **Internet Corporation for Assigned Names and Numbers (ICANN)**, vertreten durch den Präsidenten, Herrn Göran Marby, 12025 Waterfront Drive, Suite 300, Los Angeles, CA 90094-2536, USA,

- Antragstellerin -

Verfahrensbevollmächtigte:

JONES DAY Rechtsanwälte,

Neuer Stahlhof, Breite Straße 69, 40213 Düsseldorf

gegen

die **EPAG Domainservices GmbH**,   


- Antragsgegnerin -

wegen:

Unterlassung, Vertrag zur Datenerhebung bei der Domainregistrierung

Streitwert:

€ 1.000.000,00 (€ 1 Million)

COMMERZBANK MÜNCHEN • KONTO-NR. 660601601 • BLZ 700 400 41 • IBAN DE93 7004 0041 0680 6016 01 • BIC COBA DEFF33 • UST/VAT REG NO DE 112010330

AL KHOBAR • AMSTERDAM • ATLANTA • BEIJING • BOSTON • BRISBANE • BRUSSELS • CHICAGO • CLEVELAND • COLUMBUS • DALLAS • DETROIT  
DUBAI • DÜSSELDORF • FRANKFURT • HONG KONG • HOUSTON • IRVINE • JEDDAH • LONDON • LOS ANGELES • MADRID  
MEXICO CITY • MIAMI • MILAN • MINNEAPOLIS • MOSCOW • MUNICH • NEW YORK • PARIS • PERTH • PITTSBURGH • RIYADH • SAN DIEGO  
EU-133095867 • SAO PAULO • SHANGHAI • SILICON VALLEY • SINGAPORE • SYDNEY • TAIPEI • TOKYO • WASHINGTON

25. Mai. 2018  
Seite 2

Wir bestellen uns zur Verfahrensbevollmächtigten der Antragstellerin und stellen für sie den **Antrag:**

im Wege der einstweiligen Verfügung, die der besonderen Dringlichkeit wegen ohne vorauslaufende mündliche Verhandlung und durch den Vorsitzenden anstelle des Prozessgerichts erlassen werden soll, es unter Androhung eines Ordnungsgeldes von bis zu € 250.000,00, es der Antragsgegnerin aufzugeben, es zu unterlassen,

als von der ICANN akkreditierter Registrar in Bezug auf jede generische Top Level Domain, die in Anlage AS 1 aufgeführt ist,

Second Level Domainnamen, anzubieten und/oder zu registrieren, ohne die folgenden Daten des Registrierenden, der einen Second Level Domainnamen über die Antragsgegnerin registrieren will, zu erheben:

Name, Postanschrift, E-Mail-Adresse, Telefonnummer und (sofern vorhanden) Faxnummer des technischen Kontakts für den jeweiligen Domainnamen;

und/oder

Name, Postanschrift, E-Mail-Adresse, Telefonnummer und (sofern vorhanden) Faxnummer des administrativen Kontakts für den jeweiligen Domainnamen.

## BEGRÜNDUNG

Die Antragstellerin ist eine gemeinnützige Organisation, die unter anderem dafür verantwortlich ist, mit diversen Gesellschaften Verträge über die operative Tätigkeit mit generischen „Top Level Domains“ abzuschließen und mit weiteren Gesellschaften, die für die Registrierung von „Second Level Domains“ innerhalb dieser Top Level Domains verantwortlich sind. Eine generische Top Level Domain ist die Endung nach dem letzten Punkt einer Internetadresse, wie zum Beispiel „.com“ oder „.org“. Eine Second Level Domain ist der Name vor diesem letzten Punkt, wie zum Beispiel das „icann“ in „icann.org“.

Die Aufgabe der Antragstellerin ist „die stabile und sichere Funktionsweise des eindeutigen Identifikationssystems des Internets sicherzustellen“. Die Möglichkeit der Identifizierung der Inhaber der jeweiligen Kennungen gehört dabei zu den Hauptaufgaben der Antragstellerin.

Diese Hauptaufgabe der Sicherstellung einer stabilen und sicheren Funktion des Systems der eindeutigen Kennungen hat zu den Verpflichtungen im Zusammenhang mit der Bereitstellung des „WHOIS“ Services geführt. Diese Verpflichtungen sind in den Verträgen der Antragstellerin und Konsensleitlinien (die in die Verträge integriert werden) enthalten, die die Antragstellerin mit Registrars und Registries abgeschlossen hat. Diese Leitlinien und vertraglichen Verpflichtungen betreffen die Erhebung, Verwahrung, Sicherung, Übertragung und Veröffentlichung von WHOIS Registrierungsdaten, welche Kontaktinformationen von natürlichen und juristischen Personen wie auch technische Informationen in Bezug auf eine Domainregistrierung enthalten. Durch diese Leitlinien und Verträge setzt die Antragstellerin die Minimum Standards für WHOIS, wodurch die Verfügbarkeit von WHOIS Informationen gewährleistet wird, um das Risiko von Angriffen zu reduzieren, welche die stabile und sichere Funktion des Internets gefährden und um weitere öffentliche Interessen zu wahren.

Viele der Registrars und Registries haben Bedenken, ob die Leitlinien und Verträge der Antragstellerin, die sie zur Erhebung, Erstellung, Sicherung, treuhänderischen Verwaltung und Publikation von bestimmten Daten in Zusammenhang mit der Tätigkeit der Registrars oder Registries, Domainregistrierungen und Registrierenden verpflichtet, mit der heute in Kraft tretenden Datenschutzgrundverordnung (DSGVO) im Einklang stehen.

Die Antragsgegnerin ist ein „Akkreditierter Registrar“ der Antragstellerin. Das heißt, dass die Antragsgegnerin im Wege einer vertraglichen Vereinbarung mit der Antragstellerin befugt ist, Second Level Domains unterhalb einer (durch separaten Vertrag) durch die Antragstellerin vergebenen Top Level Domain zu registrieren. Wie vorstehend erläutert, ist eine der Vertragspflichten der Antragsgegnerin die Erhebung und Speicherung bestimmter erforderlicher Registrierungsdaten der Kunden.

Die Antragsgegnerin ist nunmehr der Meinung, dass sie mit dem 25. Mai 2018 aufgrund der Datenschutzgrundverordnung (DSGVO) keine Daten in Bezug auf den technischen und den

administrativen Kontakt als Teil der Kundendaten mehr erheben darf, obwohl dies in dem Vertrag mit der Antragstellerin vorgegeben ist.

Diese Ansicht geht fehl. Der technische Kontakt und der administrative Kontakt haben wichtige Funktionen. Der Zugang zu diesen Daten ist für den stabilen und sicheren Betrieb des Domain Name Systems notwendig, und er begründet die Möglichkeit, solche Kunden und Teilnehmer zu identifizieren, die technische und rechtliche Probleme mit dem Domainnamen verursachen. Die Bestimmungen der DSGVO hindern die Antragsgegnerin daher nicht daran, diese Daten zu erheben. Werden die geforderten Daten des technischen und des administrativen Kontakts von der Antragsgegnerin nicht erhoben, wird die legitime Verwendung dieser Daten, etwa durch Strafverfolgungsbehörden, die einen das Domain Name System verwendenden Straftäter lokalisieren wollen, gefährdet.

Entsprechend hat die Antragstellerin versucht, die Antragsgegnerin davon zu überzeugen, dass sie weiterhin vertraglich verpflichtet ist, die Informationen des technischen und des administrativen Kontakts zu erheben. Die Parteien waren nicht in der Lage, diese Sache außergerichtlich zu lösen. Die Antragstellerin bittet daher das Gericht, die Antragsgegnerin im Wege der einstweiligen Verfügung aufzugeben, Domainnamen nicht weiter anzubieten oder zu registrieren, ohne die erforderlichen Daten während der Registrierungsvorgangs zu erheben.

## **A. Sachverhalt**

### **I. Die Parteien**

Die **Antragstellerin** ist eine gemeinnützige Organisation, unter vielen anderen Dingen ist sie für die vertragliche Gestaltung mit Gesellschaften zum Betrieb von Top Level Domains verantwortlich sowie für die vertragliche Gestaltung mit Gesellschaften, die für die Registrierung von Second Level Domains unterhalb dieser Top Level Domains verantwortlich sind. Wir fügen eine vollständige Liste der Top Level Domains, welche die Antragstellerin vertraglich vergibt bei als

- Anlage AS 1 -.

Das Ziel der Antragstellerin ist "[...] den stabilen und sicheren Betrieb des Unique Identifier Systems für das Internets sicherzustellen [...]". Da eine der Hauptaufgaben der Antragstellerin darin besteht, für die Kennungen im Internet verantwortlich zu sein, ist die Erleichterung der Identifizierung der Inhaber der Kennungen eine Kernfunktion des Antragstellers.

Wie bereits oben ausgeführt, hat dieses Ziel zu den Verpflichtungen im Zusammenhang mit der Bereitstellung eines „WHOIS“-Services geführt, welche Bestandteil der Konsensleitlinien der Antragstellerin sowie der Verträge zwischen der Antragstellerin und den Registries und Registrars, einschließlich der Antragsgegnerin, ist. Diese Leitlinien und vertraglichen Ver-

pflichtungen regeln die Erhebung, Aufbewahrung, Treuhand, Übertragung und Zugänglichmachung von WHOIS Registrierungsdaten für Domain Namen unter einer generischen Top Level Domain. Dies beinhaltet Kontaktdaten einer natürlich oder juristischen Person sowie administrative und technische Informationen im Zusammenhang mit der Domainregistrierung. Mittels dieser Leitlinien und Verträge hat die Antragstellerin Mindestanforderungen für das WHOIS geschaffen und dadurch die Verfügbarkeit von WHOIS Informationen sichergestellt, um Angriffe, welche die stabile und sichere Funktionsfähigkeit des Internets gefährden zu minimieren.

Wir reichen Auszüge aus dem Internetauftritt der Antragstellerin mit einer kurzen Erläuterung des Aufbaus und der Aufgaben der Antragstellerin ein als

- Anlage AS 2 -.

Die **Antragsgegnerin** ist ein deutscher Anbieter von Dienstleistungen im Zusammenhang mit der Beantragung und Registrierung von Domains unter mehr als 900 Top Level Domains von länderspezifischen Top Level Domains bis hin zu neuen generischen Top Level Domains. Die Antragsgegnerin bietet auch weitere Dienstleistungen rund um die Registrierung von Domains an, wie z.B. Domain-Backordering oder die Verwaltung einer Reihe von Domainbeantragungsverfahren. Wir reichen Auszüge aus dem Internetauftritt der Antragsgegnerin, die sich auf ihren Domainregistrierungsservice beziehen, ein als

- Anlage AS 3 -.

## II. Das Registrar Accreditation Agreement zwischen den Parteien

Die Antragstellerin und die Antragsgegnerin haben am 22. Januar 2014 die als "Registrar Accreditation Agreement" bezeichnete Registrar Akkreditierungsvereinbarung (nachfolgend "RAA") unterzeichnet. Wir fügen das RAA nebst deutscher Übersetzung der maßgeblichen Abschnitte bei als

- Anlage AS 4 -.

Gemäß den Bestimmungen des RAA ist die Antragsgegnerin "akkreditiert durch ICANN als Registrar zu handeln, einschließlich in der Registrierungsdatenbank Domainnamen hinzuzufügen oder zu verlängern". Mit anderen Worten: Die Antragsgegnerin ist von der Antragstellerin bevollmächtigt, neue Domainregistrierungsvereinbarungen mit Kunden abzuschließen, die eine Second Level Domain unterhalb einer Top Level Domain erlangen möchten. Als Teil des Registrierungsprozesses war und ist die Antragsgegnerin verpflichtet, bestimmte Daten des Registrierenden an den Registerbetreiber, welcher die Registrierungsdatenbank für die jeweilige Top Level Domain unterhält, weiterzugeben.

Gemäß Ziffer 3.4 RAA hat der Registrar relevante Daten sicher in einer elektronischen Datenbank zu verwahren. Diese Verpflichtung schließt ausdrücklich die in den Ziffern 3.3.1.1 bis 3.3.1.8 des RAA bezeichneten Daten mit ein:

*„3.4.1 Für jeden durch den Registrar gesponsorten Registrierten Domainnamen innerhalb einer gTLD muss der Registrar in seiner eignen elektronischen Datenbank, die von Zeit zu Zeit aktualisiert wird, sammeln und sichern:*

*[...]*

*3.4.1.2 Die in den Ziffern 3.3.1.1. bis 3.3.1.8 aufgeführten Daten;“*

Unter den Ziffern 3.3.1.1 bis 3.1.1.8 sind die folgenden Daten in Bezug auf alle aktiven registrierten Domainnamen aufgeführt:

*3.3.1.1 Den Namen des Registrierten Domainnamens;*

*3.3.1.2 Die Namen des ersten Namensserver und des zweiten Namensserver für den Domainnamen;*

*3.3.1.3 Die Identität des Registrars (dieser kann durch die Internetseite des Registrars zur Verfügung gestellt werden)*

*3.3.1.4 Das Datum der erstmaligen Registrierung;*

*3.3.1.5 Das Enddatum der Registrierung;*

*3.3.1.6 Den Namen und die Anschrift des Registrierenden;*

*3.3.1.7 Den Namen, Anschrift, E-Mail Adresse, Telefonnummer und (soweit verfügbar) die Faxnummer des technischen Kontakts für den registrierten Domainnamen; und*

*3.3.1.8 Den Namen, Anschrift, E-Mail Adresse, Telefonnummer und (soweit verfügbar) die Faxnummer des technischen Kontakts für den registrierten Domainnamen.*

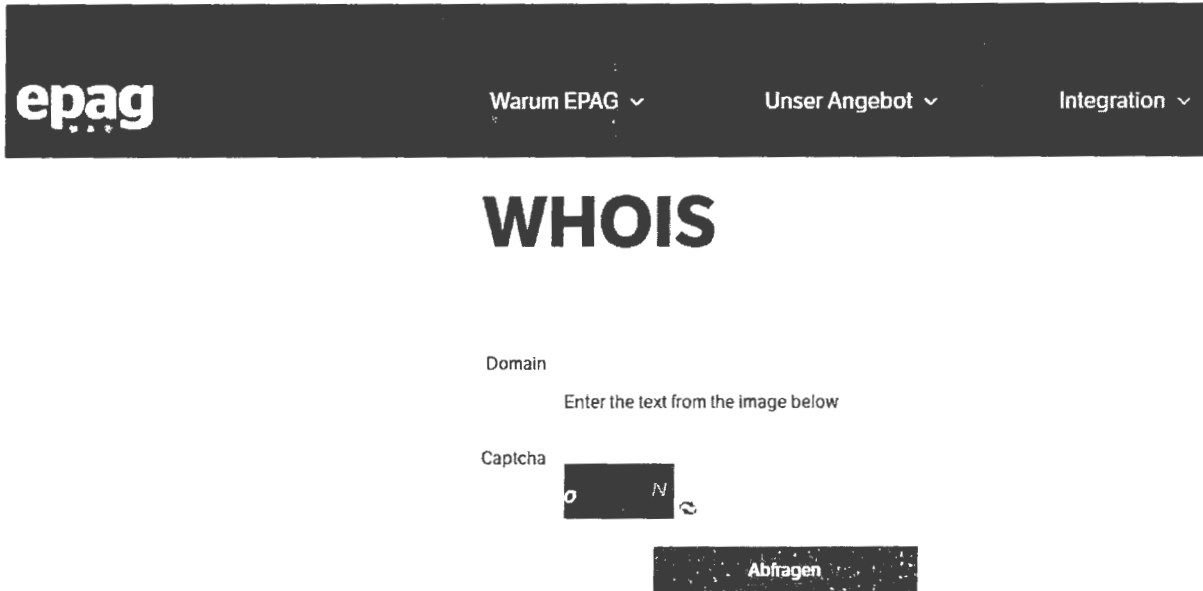
Am 17. Mai 2018 hat der Vorstand der Antragstellerin eine "Temporary Specification" (Spezifizierung für eine Übergangszeit) verabschiedet, ein einheitliches Zwischenmodell zur Gewährleistung eines gemeinsamen Rahmens für Registrierungsdatenverzeichnisse oder "WHOIS"-Daten, das nicht gegen die DSGVO verstößt. Die „Temporary Specification“ hat die Verpflichtungen der Antragsgegnerin gemäß dem RAA in Bezug auf die Erhebung und Speicherung der WHOIS Daten nicht verändert, sondern bekräftigte die Anforderungen vielmehr. Dies wird näher erläutert unter dem Abschnitt VIII 1.

### **III. Das WHOIS System**

Diese Daten werden in ein Datenbanksystem für die jeweilige Top-Level-Domain, unter der der jeweilige Second Level Domainname registriert ist, eingespeist. Dieses Datenbanksystem für eine Top Level Domain ist allgemein als „WHOIS“ bekannt. WHOIS ist keine zentral verwaltete Datenbank. Vielmehr werden die Registrierungsdaten an verschiedenen Orten gespeichert und durch eine Vielzahl von Registrars und Registries verwaltet. Diese legen ihre eigenen

Konventionen unter Beachtung der mit der Antragstellerin vereinbarten Mindestanforderungen fest.

Beispielhaft blenden wir die unter [www.epag.de/whois/](http://www.epag.de/whois/) abrufbare WHOIS Suchmaske der Antragstellerin ein:



Wir fügen weiterhin Auszüge einer Suche nach der Domain der Antragstellerin, icann.org, bei als

- Anlage AS 5 -.

WHOIS ist eine dezentralisierte Datenbank, die jedem, von Strafverfolgungsbehörden über Freiwillige zur Missbrauchsbekämpfung bis hin zu den Inhabern geistiger Eigentumsrechte und Endnutzern, die Möglichkeit bietet, Kontaktinformationen von Personen zu erhalten, die Internetressourcen wie Domainnamen und Internetprotokoll- oder "IP"-Adressen registriert halten.

Der Service, den das WHOIS-System bietet, ist von wesentlicher Bedeutung, insbesondere für diejenigen, die mit Markenangelegenheiten befasst sind oder versuchen, Betrug und Missbrauch zu bekämpfen. Die Möglichkeit, die WHOIS-Informationen zu erhalten, ist entscheidend, um die Verfügbarkeit eines Domainnamens zu überprüfen und Personen aufzuspüren, die an Markenverletzungen oder dem Missbrauch dieser Ressourcen wie Phishing, Spam oder Betrug durch missbräuchliche Markenbenutzung beteiligt sind. Der Auftrag des Antragstellers, die Sicherheit und Stabilität des Betriebs des Systems der eindeutigen Kennungen im Internet zu gewährleisten, hat zu den Verpflichtungen geführt, die mit der Erhebung und Bereitstellung von WHOIS Daten verbunden sind und die den Parteien auferlegt werden, mit denen die Antragstellerin Verträge hat.

WHOIS ist hierbei notwendig für das Management und die Sicherheit des Domain Name Systems aus folgenden, nicht abschließend aufgeführten, Gründen:

### **1. Benachrichtigung von Betrugsopfern**

Wird eine Webseite kompromittiert oder ein ehemals seriöser E-Mail Server beginnt Spam zu versenden, stellen die WHOIS Informationen Ermittlern und Strafverfolgungsbehörden Informationen zur Verfügung, um das Opfer zu kontaktieren und bei der Beseitigung zu unterstützen. WHOIS Informationen werden auch genutzt, um Organisationen, deren Systeme mit einem Virus infiziert wurden, insbesondere wenn sie hierdurch zum Bestandteil eines „Botnets“ wurden, in Kenntnis zu setzen. In solchen Fällen des Angriffs oder des Missbrauchs, welche die Sicherheit des System gefährdet, ist der umgehende Erhalt der notwendigen Informationen der erste wichtige Schritt, um Risiken zu reduzieren.

### **2. Zuordnung von strafbaren Handlungen**

WHOIS Daten sind wesentliche Informationen im Rahmen der Bekämpfung von Onlinekriminalität. So können die Informationen aus dem WHOIS System als Stichworte zur Suche in anderen Datenbanken eingesetzt werden, etwa die IP Adresse des Namensservers innerhalb des Domain Name Systems oder E-Mail Adressen in Datenbanken einer Anti-Spam Organisation. Dies kann Strafverfolgungsbehörden helfen, ein besseres Bild über die Aktivitäten von Kriminellen zu erlangen. Es hilft Strafverfolgungsbehörden dabei, sowohl die Kriminellen zu identifizieren als auch weitere Erkenntnisse über ihre Aktivitäten zu erlangen.

### **3. Verfügbarkeit von Domainnamen**

Das WHOIS gibt Auskunft darüber, ob ein bestimmter Domainname bereits registriert ist oder nicht. So können Marktteilnehmer mit dem WHOIS prüfen, welcher Domainname noch verfügbar ist und Teil einer neuen Markenstrategie werden kann.

### **4. Geltendmachung von IP-Rechten gegen Domaininhaber und beteiligte Personen**

Die Möglichkeit, den Inhaber einer markenrechtsverletzenden Domainregistrierung zu identifizieren, ist heute eine weitere Anwendung des WHOIS-Systems. In einigen Fällen werden Marken, die als Domainnamen verwendet werden, registriert, um "Phishing" zu erleichtern, oder zum betrügerischen Versands von E-Mails, die angeblich von seriösen Unternehmen stammen, um Einzelpersonen dazu zu bewegen, persönliche Informationen wie Passwörter und Kreditkartennummern preiszugeben. In anderen Fällen ist die Verwendung einer Marke in einem Domainnamen etwas weniger schwerwiegend – Marken



eines Dritten werden als Domain registriert und können Verwechslungsgefahr verursachen. In beiden Fällen schafft der Umstand, die mit diesen Domainnamen verbundenen Kontaktinformationen erhalten zu können, den Inhabern des geistigen Eigentums die Möglichkeit, sich mit den Personen, die den Domainnamen registriert haben, in Verbindung zu setzen, um die Verletzung geltend zu machen.

#### **IV. Erforderliche Daten für Domainanmeldungen – Warum die Informationen notwendig für diese Zwecke sind**

Die gemäß der Ziffern 3.3.1.1-8 RAA zu erhebenden Daten beziehen sich auf die relevanten Personen, die an der Registrierung und Verwaltung der Domains beteiligt sind und somit die Funktionsfähigkeit des Domain Name Systems sicherstellen.

Die Antragsgegnerin stellt in Frage, ob die Daten des technischen Kontakts oder **Tech-C** (3.3.1.7 RAA) und des administrativen Kontakts oder **Admin-C** (3.3.1.8 RAA) erforderlich für die Zwecke des vorstehend beschriebenen Domainsystems sind. Die Antragsgegnerin hat ihren Standpunkt mitgeteilt, dass sie aufgrund der Vorschriften der DSGVO die Daten für den Tech-C und Admin-C nicht weiter sammeln muss.

Die Daten des Tech-C und des Admin-C sind jedoch essentieller Bestandteil des Domainsystems der Antragstellerin (dazu nachfolgend unter 1. und 2.). Zudem sind die Kunden nicht einmal verpflichtet, personenbezogene Daten für den Tech-C oder den Admin-C anzugeben (dazu unter 3.).

Im Einzelnen:

##### **1. Tech-C – für das Domainsystem erforderliche Daten**

Der Tech-C ist die maßgebliche Kontaktperson im Falle von technischen Problemen im Zusammenhang mit einem Domainnamen.

Die Position des Tech-C wurde geschaffen um sicherzustellen, dass die Registrierenden eine Person, ein Unternehmen oder einen Account Manager, der auf einen anderen Bezug nimmt, identifizieren können mit der Kompetenz, technische Probleme in Bezug auf den Domainnamen zu lösen. Außerdem wurde diese Position geschaffen, um Registrierenden zu ermöglichen, diese Rolle delegieren können, sei es an a) einen IT-Experten innerhalb des Unternehmens oder b) einen auf technische Serviceleistungen spezialisierten Dienstleister.

In der Praxis ist der Tech-C mit dem Domaininhaber vertraglich verbunden, er hat Zugriff auf die Domain und ist verantwortlich für die Behebung von technischen Problemen mit dem Domainnamen.

Die Tech-C Rolle vereinfacht daher die Lösung technischer Probleme. Im Falle, dass der Registrierende eine juristische Person ist und keine abweichenden Angaben für den Tech-C gemacht wurden, wäre der Ansprechpartner bei technischen Problemen der angegebene Vertreter der juristischen Person. Insbesondere bei größeren Unternehmen kann dies die Behebung von technischen Problemen erheblich verzögern, wenn zunächst der Vorstand bzw. die Geschäftsführung kontaktiert werden müsste. Auch im Falle einer Einzelperson mag es vorteilhaft sein, einen Dritten mit der Tech-C Rolle zu beauftragen, etwa wenn der Registrierende unerfahren in technischen Angelegenheiten ist.

Das RAA verlangt, dass der Registrar die folgenden Daten für den Tech-C erhebt:

- Name
- Adresse
- E-Mail Adresse,
- Telefonnummer
- und (soweit verfügbar) Faxnummer

Diese Daten sind erforderlich, um den Tech-C zu bestimmen und geeignete Kontaktmöglichkeiten zu eröffnen. Insbesondere eine E-Mail Adresse und eine Telefonnummer sind erforderlich. Es gibt eine Vielzahl von Gründen, weshalb eine umgehende Kontaktaufnahme mit dem Tech-C erforderlich ist. Ist etwa eine Domain Name mit einem Webserver verbunden, der Gegenstand eines Cyberangriffs war und diesen mit schadhaftem Code infiziert hat, welcher nunmehr auch die Besucher der Domain infiziert, ist unverzügliches Handeln notwendig. Kommunikation über den Postweg oder selbst über E-Mail kann eine zu große Verzögerung bedeuten, um Schäden bei einer Vielzahl von Internetsutzern zu verhindern.

## **2. Admin-C - für das Domainnamenssystem erforderliche Daten**

Der Admin-C ist eine natürliche oder juristische Person, welche mit der administrativen Kontrolle, einschließlich Zugriffsrechten auf den Domainnamen, der Veränderung der Kontaktdaten und sogar der Übertragung des Domainnamens auf einen anderen Registrar oder Registranten, beauftragt ist. Mithin ist der Admin-C eine umfassend bevollmächtigte Person und für alle administrativen oder rechtlichen Fragen im Zusammenhang mit der Domain zuständig. Die Möglichkeit, einen Admin-C benennen zu können, stellt eine wichtige und legitime Möglichkeit für den Registrierenden dar, Aufgaben im Zusammenhang mit der Registrierung und der Nutzung des Domainnamens an geeignete Personen innerhalb oder außerhalb seines Unternehmens zu vergeben.

Der Registrierende ist nicht in allen Fällen die geeignete Person, sich mit den regelmäßig anfallenden Aufgaben im Zusammenhang mit einer Domain zu befassen. Während der

Registrierende die Wahl hat, selbst als Admin-C zu fungieren, kann er diese Rolle an eine geeignetere Person übertragen.

Die Rolle und die damit zusammenhängenden Aufgaben des Admin-C sind nicht nur in der Praxis sondern auch von deutschen Gerichten anerkannt. Deutsche Gerichte betrachten den Admin-C als eine Art „Hausmeister“ der Domain, der sicherzustellen hat, dass berechnigte Aufforderungen zur Löschung rechtsverletzender Inhalte unter dem Domain Namen befolgt werden (st. Rspr. BGH GRUR 2012, 304 – Störerhaftung des Admin-C bei Verletzung besonderer Prüfpflichten; OLG München BeckRS 9989, 52174 – *inter-shopping.com*). Der Admin-C ist daher nicht nur verpflichtet seine vertraglichen Pflichten gegenüber dem Domaininhaber zu befolgen. Der Admin-C ist auch gegenüber Dritten für die rechtskonforme Benutzung der Domain verantwortlich und ggf. haftbar.

Die Notwendigkeit sich durch einen Admin-C vertreten lassen zu können wird umso deutlicher, wenn man die Zahl der Top Level Domains und rechtlichen Vorschriften betrachtet, die zu beachten sind. Würde man die Zulässigkeit des Admin-C auf Grundlage des Datenschutzes verneinen, hätte der Domaininhaber nicht mehr die Möglichkeit, Aufgaben zu delegieren. Er müsste vielmehr die gesamte Domain übertragen, etwa durch eine Treuhandvereinbarung, um diese Aufgaben zu übertragen.

Die Veröffentlichung, dass ein Domaininhaber die Rolle des Admin-C einer bestimmten Person übertragen hat, ist eine essentielle Information für die Antragstellerin und jeden Dritten, der mit der Domain oder unter ihr abrufbaren Inhalten in Berührung kommt. Vor diesem Hintergrund bestehen keinerlei Zweifel daran, dass diese Rolle und die Erhebung der zugehörigen Daten auf berechtigten Interessen basiert.

Dies wird auch durch einen Vergleich mit den weltweiten Markenregistern bestätigt. Das Europäische Markenregister ermöglicht, dass jeder Markeninhaber einen rechtlichen Vertreter benennt, über den die Kommunikation mit dem Markeninhaber läuft. Das Ziel ist, dass jeder Markeninhaber durch einen Spezialisten unterstützt wird, welcher mit den Pflichten nach dem europäischen Markenrecht vertraut ist. Ferner können das Europäische Markenamt (EUIPO) und Dritte Schriftstücke an den rechtlichen Vertreter zustellen. Der rechtliche Vertreter sowie auch der Admin-C erfüllen damit maßgebliche Funktionen in den jeweiligen Systemen.

### **3. Welche Daten werden in Bezug auf den Tech-C und Admin-C gesammelt?**

Im Rahmen der Beurteilung der Erhebung und Verarbeitung der Daten für den Tech-C und Admin-C, nämlich Name, Adresse, E-mail Adresse, Telefonnummer, und (soweit verfügbar) Faxnummer, muss ferner das nachfolgende berücksichtigt werden:

- (1) Es besteht keine Verpflichtung, dass der Tech-C eine natürliche Person ist. Im Gegenteil, er kann eine juristische Person oder eine Referenz zu einem Account Manager sein; und
- (2) Der Tech-C darf auch dieselbe natürliche oder juristische Person sein wie der Domaininhaber.

Sofern die Daten für den Tech-C oder Admin-C personenbezogene Daten darstellen (und damit der DSGVO unterfallen), gibt es zwei Kategorien an Daten:

- (i.) die Daten sind identisch mit den Daten des Domaininhabers; und
- (ii.) die Daten weichen von den Daten für den Domaininhaber ab.

Im **ersten Fall** werden überhaupt keine "neuen" Daten erhoben. Würden überhaupt keine Tech-C oder Admin-C Daten erhoben, müssten alle Anfragen unmittelbar an den Domaininhaber gerichtet werden; also im Falle einer juristischen Person an deren gesetzlichen Vertreter. In diesem Fall werden überhaupt keine zusätzlichen personenbezogenen Daten erhoben.

Im **zweiten Fall**, d.h. wenn der Domaininhaber sich entschließt, eine andere Person als sich selbst anzugeben und die Daten personenbezogene Daten darstellen, sind diese Daten einer Prüfung nach der DSGVO unterworfen und werden im Rahmen der rechtlichen Würdigung bewertet. Aber die Antwort hierzu lautet, dass die DSGVO nicht bezweckt, Kontaktdaten, welche essentieller Bestandteil eines wichtigen und anerkannten Systems sind und berechtigten und wichtigen Zwecken dienen, künftig nicht mehr erheben zu dürfen bzw. diese löschen zu müssen.

## V. Vergleich zwischen WHOIS System und Markenregistern

Diese Funktionen und Inhalte der WHOIS Datenbanken sind gut vergleichbar mit einem Markenregister, wobei das Domain System Bezug zum Internet hat, was zu weiteren Herausforderungen führt:

### 1. Markenregister

Mit dem internationalen Abkommen über „Trade-Related Aspects of Intellectual Property Rights“ (TRIPS) haben alle relevanten Ökonomien der Welt sich auf ein bestimmtes Schutzlevel in Bezug auf bestimmte Rechte an geistigem Eigentum geeinigt, einschließlich der Marken. Dadurch hat grundsätzlich jedes Markensystem, das auf TRIPS basiert sein eigenes Markenregister, welches folgende gesammelte Informationen beinhaltet:

#### a. Inhalt eines Markenregisters

Das Europäische Markenregister zeigt alle relevanten Daten in Bezug auf eine registrierte europäische Marke, einschließlich personenbezogener Daten des Inhabers und eines (teils vorgeschriebenen) Vertreters, der den Inhaber vertritt, einschließlich aller Kontaktdaten (Adresse, Telefonnummer, Faxnummer und Email), der Korrespondenz und gerichtlicher Entscheidungen in Zusammenhang mit der Markenmeldung.

Als Beispiel fügen wir hier eine Kopie der Markenmeldung EUTM 002886448 DOPO-DOPO und die zu Grunde liegende Information bei als

- Anlage AS 6 -.

Wenn man diese Inhalte mit WHOIS vergleicht, ist festzuhalten, dass im Wesentlichen dieselben personenbezogenen Daten erhoben werden, wobei a) der Markeninhaber einen rechtlichen Vertreter benennt, der die Kommunikation und rechtliche Themen übernimmt und b) der Domaininhaber auf einen Tech-C und einen Admin-C verweisen kann, die sich um technische und administrative Dinge kümmern.

#### **b. Funktion des Markenregisters**

Das Markenregister, das im Wesentlichen dieselben Informationen beinhaltet wie WHOIS hat auch im Wesentlichen dieselben Funktionen:

##### **i. Rechtsdurchsetzung durch staatliche Stellen – Opferschutz und die Zu rechnung von Straftaten**

Das Markenregister hilft den staatlichen Stellen, zum Beispiel während Untersuchungen hinsichtlich Verkaufs von gefälschten Produkten. Das Markenregister zeigt den berechtigten Markeninhaber und vereinfacht eine Identifikation und Kontaktaufnahme mit Verdächtigen oder Parteien, die von Betrug oder Markenverletzungen betroffen sind.

Diese Funktion deckt sich im Wesentlichen mit dem WHOIS System, bei dem die vom Betrug im Internet Betroffenen Personen via WHOIS umgehend identifiziert und kontaktiert werden können.

##### **ii. Verfügbarkeit einer Marke**

Beide Register ermöglichen den Marktteilnehmern, die Verfügbarkeit bestimmter Zeichen zwecks zukünftiger Benutzung zu prüfen. Und die Marktteilnehmer sind in der Lage, in Bezug auf bestimmte Marken oder Domains Informationen zu den an der Registrierung beteiligten Personen einzuholen.

### iii. Durchsetzung von Markenrechten

Das Markenregister hat außerdem den wichtigen Zweck, Marktüberwachung zu ermöglichen. Die Gerichte fordern von Markeninhabern solche Marktüberwachung durchzuführen, um nicht das Recht zu verlieren, ihre Marke durchzusetzen (vgl. BGH GRUR 2016, 705, 709). Und die Markeninhaber müssen in der Lage sein, zu erforschen, ob weitere Markenrechte im Markt existieren, um die Risiken einer Markenverletzung einzuschätzen.

Das WHOIS System dient daher im Wesentlichen demselben Zweck, wobei der Inhalt des Markenregisters zu Daten und weiteren Informationen sehr viel weitergehend ist, als derjenige des WHOIS Systems für Domain Namen.

## 2. Marken und Domain Namen

Wie bereits dargelegt haben Marken und Domain Namen dieselbe Funktion Angebote und Waren und Dienstleistungen im Markt unterscheiden zu können.

Die rechtliche Grundlage von Marken und Domain Namen ist jedoch unterschiedlich. Marken sind ein konstitutiver Teil eines jeden Rechtssystems, das auf TRIPS basiert. Hierdurch haben alle TRIPS Vertragsstaaten Markengesetze umgesetzt, die explizite Regelungen zu den markenrechtlichen Verfahren und zum sicheren und stabilen Betrieb eines Markenregisters beinhalten.

Die Situation bei Domains ist hier gänzlich anders. Das Domain Namen System oder „DNS“ ist ein dezentralisiertes Namenssystem für Computer, Services oder andere Ressourcen, die an das Internet angeschlossen sind. Das Bestehen und die Erhaltung des Domain Namen Systems basiert nicht auf internationalen Staatsverträgen sondern vielmehr auf vertraglichen Vereinbarungen zwischen den involvierten Parteien.

Nichtsdestotrotz steht der Nutzen und die Existenz und die Funktionen des Domain Namen Systems außer Frage. Und die Gerichte finden einen Weg, die nötigen Rechte und damit verbundenen Verpflichtungen dem DNS zuzuschreiben, sei es durch die Auslegung des Rechts, im Wege der analogen Anwendung des Rechts oder durch die Entwicklung des Rechts.

## VI. Die Umsetzung der DSGVO

Am 14. April 2016 hat die Europäische Union (EU) die Datenschutzgrundverordnung verabschiedet, die am 25. Mai 2018 in Kraft tritt. In Deutschland löst sie das BDSG ab. Gemäß der Europäischen Kommission ist das Ziel der DSGVO, alle EU Bürger und hier lebende Personen

vor Verletzungen ihrer Privatsphäre und Datenschutzverletzungen zu schützen. Sie findet auf alle Unternehmen Anwendung, die personenbezogene Daten von Datenschutzsubjekten in der EU verarbeiten oder speichern.

Die DSGVO erlaubt die Erhebung und die Verarbeitung von personenbezogenen Daten nur für bestimmte Zwecke (Art. 5 (1) lit. b DSGVO), welche von der Person, die für die Daten verantwortlich ist, bestimmt werden müssen. Ohne einen bestimmten Zweck anzugeben, ist die Erhebung und Verarbeitung von Daten rechtswidrig. Zudem bestimmt Art. 5 DSGVO weitere Voraussetzungen, damit eine Verarbeitung rechtmäßig ist (z. B. guter Glaube in Art. 5 (1) lit. a DSGVO und Datenminimierung in Art. 5 (1) lit. c DSGVO).

Der bestimmte Zweck ist im Hinblick auf Datenminimierung das Hauptprinzip, wenn zu bestimmen ist, welche Daten verarbeitet werden dürfen (Ehmann/Selmayr, Art. 5 Rn. 13). Wenn die Verarbeitung notwendig ist, um den legitimen Zweck zu erreichen, ist die Verarbeitung rechtmäßig nach der DSGVO. Der Zweck muss eindeutig sein, damit die betroffene Person darüber informiert ist, warum die Daten verarbeitet werden (vgl. auch Art. 13 und 14 DSGVO, die bestimmen welche Informationen dem Berechtigten zur Verfügung gestellt werden müssen, wenn Daten verarbeitet werden).

Zudem beschreibt Art. 6 DSGVO unter welchen Umständen eine Erhebung und Verarbeitung erlaubt ist. Hierzu gehört unter anderem die Einwilligung (Art. 6 (1) lit. a DSGVO), die Erforderlichkeit für die Erfüllung eines Vertrags (Art. 6 (1) lit. b DSGVO), die Erforderlichkeit für die Erfüllung einer sonstigen rechtlichen Verpflichtung (Art. 6 (1) lit. c DSGVO) und – besonders relevant – berechnete Interessen an der Verarbeitung, wenn die Interessen der betroffenen Person nicht überwiegen (Art. 6 (1) lit. f DSGVO). Die Interessenabwägung hat durch den Verantwortlichen zu erfolgen (Ehmann/Selmayr, Art. 6 Rn. 27).

## **VII. Kein Einfluss der DSGVO auf Markenregister**

Das Inkrafttreten der DSGVO am 25. Mai 2018 hat keinen Einfluss auf die Erhebung und Publikation personenbezogener Daten in Markenregistern. Alle oben erwähnten Daten werden weiter erhoben und veröffentlicht, zugänglich für Personen innerhalb und außerhalb der EU. Der Grund hierfür ist recht einleuchtend. Die Staaten haben rechtliche Vorschriften erlassen, die das Sammeln und Speichern dieser Daten vorsehen. Diese Rechtsvorschriften implizieren die Notwendigkeit der Datenerhebung. Folglich stellt die DSGVO diese Datenerhebung nicht in Frage.

## **VIII. Einfluss der DSGVO auf das WHOIS System**

Im Hinblick auf das WHOIS System hingegen, haben viele Experten aus der Domain Industrie ihre Ansicht dargetan, dass das Inkrafttreten der DSGVO weitreichende Änderungen nach sich ziehen muss. Ihr Argument ist im Wesentlichen, dass bestimmte Daten, die im Rahmen der

WHOIS Datenbank gesammelt werden nicht notwendig sind, um legitime Zwecke zu erreichen. Diese Bedenken richten sich hauptsächlich gegen die Veröffentlichung der Daten und wie diese erfolgt.

## 1. Die Implementierung der Temporären Spezifikation durch ICANN

Die DSGVO hat zur Priorisierung und Dringlichkeit der Debatte über Datenschutz und Schutz der Privatsphäre im Rahmen des WHOIS Systems geführt. Und die Antragstellerin hat die Bedenken, die oben dargelegt wurden, sehr ernst genommen. Über die letzten Monate hat sie Rücksprache gehalten mit Stakeholders, Vertragsparteien, Europäischen Datenschutzbehörden, rechtlichen Experten und interessierten Regierungen, um den potentiellen Einfluss der DSGVO auf die Erhebung, Darstellung und Verarbeitung der personenbezogenen Daten im Rahmen des gTLD Domain Namen Systems gemäß den Verträgen und Richtlinien von ICANN zu evaluieren.

Im Ergebnis hat die Antragstellerin eine „Temporäre Spezifikation“ über die Erhebung und Nutzung von Daten im Rahmen von WHOIS Datenbanken verabschiedet. Wir reichen eine Kopie dieser Temporären Spezifikation ein als

**-Appendix AS 7-**

Wenn diese Temporäre Spezifikation am 25. Mai 2018 in Kraft tritt, wird das WHOIS System weiterhin zur Verfügung stehen, allerdings mit einigen Änderungen. Wesentlich ist, dass Registry Operators und Registrars weiterhin dazu verpflichtet sind, alle Registrierungsdaten zu erheben. Dies ist im Einklang mit den erklärten Zielen der Antragstellerin, DSGVO-konform zu handeln und dabei das bestehende WHOIS System so weit wie möglich zu erhalten.

Diese Temporäre Spezifikation bindet alle Registrars, auch die Antragsgegnerin gemäß Art. 4 RAA und den „Consensus Policies and Temporary Policies Specifications“.

Die Temporären Spezifikationen enthalten die Zwecke in Art. 4.4, für die die Datenerhebung erfolgt. *Unter anderem* werden die Rechte des Registrierenden oder „Registered Name Holder“ berücksichtigt (Art. 4.4.1). Ferner, dürfen Daten nur erhoben werden, um aufgrund eines legitimen Interesses, welches die fundamentalen Rechte des Datensubjekts überwiegen, den Zugang zu richtigen, verlässlichen und eindeutigen Registrierungsdaten zu ermöglichen (Art. 4.4.2), einschließlich zum Zwecke der Schaffung administrativer und technischer Ansprechpartner auf Geheiß des Registrierenden (Art. 4.4.7).

Die Temporären Spezifikationen halten auch fest, warum die Antragstellerin zu dem Schluss gekommen ist, dass die Erhebung und Verarbeitung der Daten verhältnismäßig ist (Art. 4.5). Sie bestimmen außerdem, was der Registrar den Registered Name Holders mitteilen muss (Art. 7.1, der Art. 3.7.7.4 des RAA ersetzt).



Wenn Internetnutzer eine WHOIS Anfrage stellen, werden sie zumindest „dünne“ Daten erhalten, inklusive technischer Daten, die genügen, um den Registrar zu identifizieren, den Status der Registrierung und Zeitpunkt der Eintragung und das Ablaufdatum der Registrierung. Zudem wird der Nutzer Zugriff haben auf eine anonymisierte E-mail Adresse oder ein web Formular, um E-Mail Kommunikation mit dem entsprechenden Kontakt zu ermöglichen (z. B. Registrant, Admin-C, Tech-C). Die Antragstellerin ist aufgefordert, diese Temporären Spezifikationen auch durchzusetzen, da sie integrativer Bestandteil des RAA geworden sind.

## **2. Verpflichtungen der Registrars unter den Temporären Spezifikationen**

Folglich hat die Antragstellerin die Anforderungen der DSGVO im Rahmen der WHOIS Datenbanken umgesetzt. Und damit sind gleichzeitig die Registrars weiterhin verpflichtet, die Daten, die im RAA genannt (und in den Temporären Spezifikationen bestätigt) werden, zu erheben und zur Verfügung zu stellen.

Insbesondere muss die Antragsgegnerin weiterhin die Daten über den Tech-C und den Admin-C erheben und verwahren.

## **IX. Die Rechtsposition der Antragsgegnerin**

Die Antragsgegnerin hat ihren Standpunkt dargelegt, dass sie bei der Registrierung der Domains nicht weiter die Daten in Bezug auf den Tech-C und den Admin-C erheben sollte, da sie glaube, hiermit gegen die Vorgaben der DGSVO zu verstoßen.

Die Parteien haben diese Fragen in mehreren Telefonaten erörtert. Und die Antragstellerin hat ihre Bedenken geäußert sowie ausdrücklich erwähnt, dass sie dazu bereit ist, ein einstweiliges Verfügungsverfahren in Deutschland einzuleiten, um eine entsprechende Entscheidung eines deutschen Gerichts hierzu zu erlangen.

Ferner fand am **24. Mai 2018** eine Telefonkonferenz mit den folgenden Teilnehmern statt:

[REDACTED]  
 [REDACTED]  
 [REDACTED] John Jeffrey, General Counsel and Secretary der Antragstellerin, Amy Stathos, Deputy General Counsel der Antragstellerin; Erika Randall, Associate General Counsel der Antragstellerin [REDACTED]  
 [REDACTED]

Der Unterzeichner Jakob Guhn fasste die Sachlage zusammen und wies auf die Bedenken der Antragstellerin hin. Ferner bat er den Rechtsvertreter der Antragsgegnerin, die rechtliche Position bezüglich der angekündigten Nichterhebung von Daten ab dem 25. Mai 2018 zu erläutern.

■■■■■ bestätigte als Antwort hierauf, dass die Antragsgegnerin ab dem 25. Mai 2018 Daten zum Tech-C und zum Admin-C nicht mehr erheben werden.

Zudem wurde von ■■■■■ ausdrücklich bestätigt, dass für die Kunden der Antragsgegnerin ab dem 25. Mai 2018 die Möglichkeit bestehen wird, im Wege eines „Updates“ die Tech-C und Admin-C Daten aus dem Account der Antragsgegnerin zu registrierten Domainnamen zu löschen. Ferner sagte er während des Telefonats, dass die Antragsgegnerin derzeit an einem Plan arbeite, diese Daten systematisch zu löschen. Dieser Plan sei aber bisher noch nicht umgesetzt (dies soll aber nicht mehr der Fall zu sein, wie von John Jeffrey bestätigt und nachfolgend erläutert).

Der obig dargestellt Inhalt des Telefonats entspricht nach bestem Wissen und Gewissen des Unterzeichners den Tatsachen, was hiermit **anwaltlich versichert** wird.

In einem Folgetelefonat am selben Tag zwischen ■■■■■ und John Jeffrey hat ■■■■■ sich einverstanden erklärt, dass die Antragsgegnerin derzeit keinerlei erhobene WHOIS Daten permanent löschen wird, außer wenn dies in den ICANN Leitlinien vorgesehen ist, und er versprach, die Antragstellerin in Kenntnis zu setzen, bevor solche Maßnahmen umgesetzt werden. Auf der anderen Seite bestätigte ■■■■■ erneut, dass die Antragsgegnerin zukünftig nur noch die Daten des Registrierenden erheben wird – und nicht die Daten zum Admin-C oder zum Tech-C.

Wir legen eine entsprechende Versicherung von John Jeffrey zu diesen Aussagen vor als

**-Appendix AS 8-**

Ferner kündigte ■■■■■ an, der Antragstellerin einen Brief zuzusenden, in dem der Standpunkt der Antragsgegnerin näher erläutert wird. Bis jetzt hat die Antragstellerin aber lediglich einen „DRAFT“, einen Entwurf, erhalten. Sofern die Antragstellerin jedoch eine verbindliche Stellungnahme der Muttergesellschaft der Antragsgegnerin erhält, wird sie dieses unverzüglich an das Gericht weiterleiten.

In der Konsequenz besteht hiernach das hohe Risiko, dass die Antragsgegnerin ab dem 25. Mai 2018 die folgenden Daten, entgegen der vertraglichen Vereinbarung in Ziffern 3.3.1.7 und 3.3.1.8 des RAA, bestätigt durch die Temporary Specifications, nicht weiter erhebt:

Name, Postanschrift, E-Mail-Adresse, Telefonnummer und (sofern vorhanden) Faxnummer **des technischen Kontakts** für den jeweiligen Domainnamen;

und/oder

Name, Postanschrift, E-Mail-Adresse, Telefonnummer und (sofern vorhanden) Faxnummer **des administrativen Kontakts** für den jeweiligen Domainnamen.

## **B. Rechtliche Würdigung**

Der Antrag auf einstweilige Verfügung ist begründet. Die Antragstellerin hat einen Unterlassungsanspruch (unten I) und die Sache ist eilig, da die Antragsgegnerin angekündigt hat, Daten über den Tech-C und den Admin-C ab dem 25. Mai 2018 nicht länger zu sammeln (unten II).

### **I. Verfügungsanspruch**

Die Antragstellerin hat einen vertraglichen Anspruch gegen die Antragsgegnerin nur dann Domains zum Verkauf anzubieten, wenn die im Antrag aufgeführten Daten weiterhin erhoben und gespeichert werden.

Die Antragstellerin hat einen vertraglichen Anspruch gegen die Antragsgegnerin, die Daten wie in Art. 3.3.1.1 bis 3.3.1.8 RAA vereinbart zu verarbeiten, einschließlich der Daten des Tech-C (3.3.1.7) und des Admin-C (3.3.1.8). Außerdem hat die Antragstellerin einen Anspruch gemäß Art. 3.4.1.2 RAA, dass die Antragsgegnerin die Daten sicher speichert. Diese Verpflichtung bezieht sich auf jeden registrierten und von der Antragsgegnerin gesponserten Domainnamen, d.h. der zu der Anmeldung gehörige Datensatz wurde in das Register eingegeben, 1.26 RAA.

Trotz dieses vertraglichen Anspruchs hat die Antragsgegnerin gedroht, Daten bezüglich Tech-C und Admin-C bei neuen Registeranmeldungen umgehend nicht mehr zu sammeln. Ferner scheint die Antragsgegnerin an einem Plan zur permanenten Löschung der Tech-C und Admin-C Daten in naher Zukunft zu arbeiten. Die angebliche Grundlage für diese Nicht-Sammlung und eine etwaige Löschung ist das Inkrafttreten der DSGVO. Allerdings ändert die DSGVO an den Verpflichtungen der Antragsgegnerin nichts – sie ist weiterhin verpflichtet, die Daten zu sammeln und verwahren auf Grundlage von Art. 6 (1) lit. a und/oder Art. 6 (1) lit. f DSGVO.

Die einzigen Daten, die vorliegend im Streit stehen sind die Tech-C und Admin-C Daten, da die Antragsgegnerin anzuerkennen scheint, dass die anderen Daten von ihr weiter zu erheben und zu speichern sind. Diese jeweiligen Daten müssen aber weiterhin erhoben werden aus folgenden Gründen:

## 1. Keine personenbezogenen Daten – Keine Anwendbarkeit der DSGVO

Wie oben dargelegt, beziehen sich viele der fraglichen Daten gar nicht auf personenbezogene Daten. Die Datenschutzgrundverordnung ist allerdings:

*„zum Schutz **natürlicher** Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“ (Untertitel der DSGVO)*

erlassen worden.

Die Antragsgegnerin versucht dementsprechend die Nichterhebung von Daten bezüglich Tech-C und Admin-C zu rechtfertigen, ohne sich überhaupt damit auseinanderzusetzen, ob die entsprechenden Daten personenbezogene Daten darstellen.

## 2. Art. 6 (1) lit. a DSGVO

In dem Fall, dass die Tech-C und Admin-C Daten personenbezogene Daten darstellen, ist ihre Erhebung und Verarbeitung rechtmäßig, insbesondere auf der Basis einer Einwilligung im Sinne von Art. 6 (1) lit. a DSGVO.

Art. 6 (1) lit. a DSGVO bestimmt, dass die Verarbeitung rechtmäßig ist, wenn

*[d]ie betroffene Person [...] ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben [hat].*

Tatsächlich ist die Antragsgegnerin nach dem RAA in Verbindung mit den Temporary Specifications nicht daran gehindert, die Zustimmung des benannten Tech-C oder Admin-C einzuholen. Im Gegenteil, Ziffer 7.2 der Temporary Specifications sieht dies ausdrücklich vor:

*"7.2.2. Der Registrar DARF dem Admin/Tech und/oder anderen Ansprechpartnern die Möglichkeit geben, ihre Zustimmung zur Veröffentlichung zusätzlicher Kontaktinformationen gemäß Abschnitt 2.4 der Anlage A zu erteilen".*

Während es unklar bleibt, warum die Antragsgegnerin diese Möglichkeit nicht ausschöpft, kann die Antragsgegnerin nicht geltend machen, dass die Zustimmung von Tech-C und Admin-C gemäß Art. 7 DSGVO unwirksam wäre. Insbesondere liegt kein Verstoß gegen Art. 7 (4) DSGVO:

*„(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.“*

Die Durchführung der Registrierung des Domain Namens ist nicht von der Einwilligung abhängig. Denn wenn die Person, die als Tech-C oder Admin-C angegeben werden soll nicht einwilligt, verbleibt die entsprechende Rolle beim Registrierenden. Nach dem RAA (einschließlich der Temporary Specifications) besteht keine Verpflichtung, dass Tech-C oder Admin-C durch personenbezogene Daten identifiziert werden müssen oder überhaupt von dem Registrierenden verschieden sein müssen. Daher kann der Domainanmelder den Domain Namen erhalten, auch ohne überhaupt personenbezogene Daten anzugeben.

### 3. Art. 6 (1) lit. b DSGVO

Nach Art. 6 Abs. 1 lit. b) DSGVO ist die Verarbeitung ebenfalls zulässig, wenn und soweit:

*b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;*

Auch diese Anforderungen werden im vorliegenden Fall erfüllt.

Die Rolle des Admin-C und Tech-C ist auch eine wichtige Option für den Registranten, um Aufgaben bezüglich seines registrierten Domain Namens zu delegieren. Gemäß dem RAA muss die Antragsgegnerin solche Daten im Hinblick auf eine neue Registrierung eines Domain Namen sammeln. Die Nichterhebung der Antragsgegnerin (oder etwaige Löschung in naher Zukunft) würde es dem Registrierenden unmöglich machen, von dieser Option zu profitieren.

Daher sollte es keinen Zweifel daran geben, dass die Erhebung solcher Daten für die Erfüllung des Vertrages erforderlich ist.

### 4. Art. 6 (1) lit. f DSGVO

Darüber hinaus ist es auch im berechtigten Interesse jedweder Dritter, die bisher gesammelten Daten weiterhin zu behalten (Art. 6 (1) lit. f DSGVO). Gemäß Art. 6. (1) f DSGVO ist eine Verarbeitung von personenbezogenen Daten zulässig, wenn:

*(f) die Verarbeitung [...] zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.*

Die Antragstellerin hat im Detail dargelegt, warum es für den Registrierenden wichtig ist, Aufgaben in Bezug auf den Domainnamen an einen Tech-C oder Admin-C delegieren zu können. Diese Funktionen sind ein wesentlicher Teil des Domain Namen Systems, die sicherstellen, dass große Unternehmen und natürliche Personen ohne technisches Wissen Personen mithilfe des Namens oder einer Referenz oder Dienstleister bezeichnen können, die diese Aufgaben erfüllen können. Zudem ist die Verarbeitung von personenbezogenen Daten nicht zwingend erforderlich. Werden personenbezogene Daten verarbeitet, geht es häufig um Kontaktdetails innerhalb eines Unternehmens.

Der Vergleich mit Markenregistern zeigt auch, dass ein solches berechtigtes Interesse an der Erhebung solcher Daten nicht in Frage gestellt werden kann. Markenregister sammeln ähnliche Daten, um die Möglichkeit zu geben, Aufgaben im Zusammenhang mit der Registrierung und Pflege der Marke an einen rechtlichen Vertreter zu delegieren, der ein Experte für Markenangelegenheiten ist. Somit werden grundsätzlich die gleichen Daten für die gleichen Funktionen und Ziele erhoben. Und es wird nicht einmal diskutiert, ob eine solche Datenerhebung datenschutzrechtliche Bedenken unterworfen ist.

Die Antragstellerin hat auch die Zwecke, warum diese Daten verarbeitet werden müssen, dargelegt, wie in Abschnitt 4.1 – 4.3 der Temporären Spezifikation festgelegt:

*„Die Aufgabe der ICANN, wie in Abschnitt 1.1(a) der Satzung dargelegt, besteht darin “den stabilen Betrieb der Eindeutigen Identifizierungssysteme des Internetz zu koordinieren”. Abschnitt 1.1(a) beschreibt spezifisch, was diese Mission in Zusammenhang mit den Namen beinhaltet.*

*Die Rolle der ICANN ist zwar eng, beschränkt sich aber nicht auf die technische Stabilität. Insbesondere sieht die Satzung vor, dass die ICANN den Zweck hat, die Bottom-up-, Multistakeholder-Entwicklung und Umsetzung von Richtlinien zu koordinieren “[f]ür welche einheitliche oder koordinierte Lösung vernünftigerweise notwendig ist, um die Offenheit, Interoperabilität, Belastbarkeit, Sicherheit und/oder Stabilität des DNS zu erleichtern, einschließlich, in Bezug auf gTLD-Registrars und Registry Operators”[Satzung, Abschnitt 1.1(a)(i)], der weiter in Anhang G1 und G2 der Satzung definiert ist, um unter anderem Folgendes einzuschließen:*

- *Beilegung von Streitigkeiten im Zusammenhang mit der Registrierung von Domainnamen (im Gegensatz zur Verwendung solcher Domainnamen, aber auch, wenn diese Richtlinien die Verwendung der Domainnamen berücksichtigen);*

- *Pflege und Zugriff auf korrekte und aktuelle Informationen über registrierte Namen und Nameserver;*
- *Verfahren zur Vermeidung von Störungen bei der Registrierung von Domainnamen aufgrund der Aussetzung oder Beendigung des Betriebs durch einen Registry Operator oder einen Registrar (z.B. Escrow); und*
- *die Übermittlung von Registrierungsdaten bei einem Wechsel des Registrars, der einen oder mehrere registrierte Namen sponsert.*

*Die Satzung legt fest, dass Fragen im Zusammenhang mit der Bereitstellung von Registration Data Directory Services (RDDS) durch Registry-Betreiber und Registrars fest in den Aufgabenbereich der ICANN fallen. Die Statuten geben weitere Einblicke in die berechtigten Interessen, denen RDDS dienen soll. Beispielsweise verpflichtet die Satzung die ICANN bei der Erfüllung ihres Mandats ausdrücklich "Fragen des Wettbewerbs, des Verbraucherschutzes, der Sicherheit, der Stabilität und Widerstandsfähigkeit, des böswilligen Misbrauchs, der Souveränität und des Rechtsschutzes angemessen zu behandeln" [Statutenabschnitt 4.6 (d)]. Während die ICANN weder die Autorität noch das Fachwissen hat, um Wettbewerbs- oder Verbraucherschutzgesetze durchzusetzen, und nur einer von vielen Akteuren im Ökosystem der Cybersicherheit ist, ist die Bereitstellung von RDDS für berechnete und verhältnismäßige Nutzungen eine kritische und grundlegende Art und Weise in der die ICANN den Verbraucherschutz, Fragen des Böswilligen Missbrauchs, Souveränitätsbelange und den Schutz von Rechten anspricht – die Durchsetzung von Richtlinien, die es Verbrauchern, Rechteinhabern, Strafverfolgungsbehörden und anderen Akteuren ermöglichen, auf die erforderlichen Daten zuzugreifen, um gegen Gesetze oder Rechte verstoßende Nutzungen vorzugehen und dies zu lösen.*

*Dementsprechend beinhaltet der Auftrag der ICANN direkt die Erleichterung der Verarbeitung durch Dritte zu berechtigten und verhältnismäßigen Zwecken in Bezug auf Strafverfolgung, Wettbewerb, Verbraucherschutz, Vertrauen, Sicherheit, Stabilität, Widerstandsfähigkeit, böswilligen Missbrauch, Souveränität und Schutz der Rechte. ICANN wird von Abschnitt 4.6(e) der Satzung gefordert, vorbehaltlich der anwendbaren Gesetze, "wirtschaftlich vertretbare Anstrengungen zu unternehmen, um ihre Richtlinien in Bezug auf Registrierungsverzeichnisse durchzusetzen", einschließlich der Zusammenarbeit mit Interessengruppen, um "strukturelle Änderungen zur Verbesserung der Genauigkeit und des Zugangs zu generischen Toplevel-Domain-Registrierungsdaten zu untersuchen", "sowie Schutzmaßnahmen zum Schutz dieser Daten zu berücksichtigen". Daher ist die ICANN der Ansicht, dass die Erhebung personenbezogener Daten (eines der Elemente der Verarbeitung) durch die Satzung ausdrücklich vorgeschrieben ist. Darüber hinaus sind weitere Elemente der Verarbeitung personenbezogener Daten in Registrierungsdaten durch den Registry Operator und den Registrar erforderlich und zulässig, um einen koordinierten, stabilen und sicheren Betrieb des einzigartigen Identifizierungssystems des Internets zu gewährleisten."*

Die Antragstellerin hat ausführlich dargestellt, warum das Interesse jedweder Dritter an der Datenverarbeitung die individuellen Interessen des Betroffenen überwiegen, wenn es um die Tech-C und die Admin-C Daten geht.

Bei Abwägung der Interessen kann kein Zweifel daran bestehen, dass die Erhebung dieser Daten unter der DSGVO gerechtfertigt ist. Daher kann die Antragsgegnerin sich nicht darauf berufen, dass die DSGVO sie an der Erfüllung ihrer vertraglichen Verpflichtung gemäß dem RAA hindert.

## II. Verfügungsgrund

Die Angelegenheit ist dringend. Die Antragstellerin hat unverzüglich Schritte unternommen, als sie Kenntnis davon erlangte, dass die Antragsgegnerin sich nicht an ihre vertraglichen Pflichten halten würde und ab dem 25. Mai 2018 die entsprechenden Daten nicht länger erheben würde. Einstweiliger Rechtsschutz ist notwendig, um irreparablen Schaden abzuwenden. Mit diesem Antrag versucht die Antragstellerin zu verhindern, dass bestimmte Daten unwiederbringlich verloren gehen.

Am 14. Mai 2018 erfuhr die Antragstellerin in der Person von Herrn John Jeffrey, General Counsel und Secretary der Antragstellerin von [REDACTED] der Muttergesellschaft der Antragsgegnerin, dass die Antragsgegnerin bestimmte Daten ab dem 25. Mai 2018 möglicherweise nicht länger erheben wird.

In einem Schreiben vom 17. Mai 2018 forderte unter anderem Tucows ein Moratorium, um die Temporären Spezifikationen umzusetzen um „die Möglichkeit zu erhalten so weitgehend wie möglich die jeweilige Umsetzung der DSGVO mit den DSGVO-konformen Teilen von etwaigen Temporären Spezifikationen in Übereinstimmung zu bringen“.

In einem nachfolgenden Telefonat am 24. Mai 2018 wurde die Antragstellerin erstmals genauer über die konkreten Pläne der Antragsgegnerin informiert. Entsprechend eilig ist diese Sache.

Die Nichterfüllung ihrer vertraglichen Verpflichtungen durch die Antragsgegnerin würde irreparablen Schaden nach sich ziehen. Denn sobald die Antragsgegnerin die Daten nicht länger erhebt, sind sie unwiederbringlich verloren. Um Unsicherheiten bezüglich des derzeitigen WHOIS-Systems Rechnung zu tragen, hat die Antragstellerin die Temporären Spezifikationen erlassen. Hiernach ist die Antragsgegnerin zwar nicht verpflichtet, die Daten über Tech-C und Admin-C öffentlich zugänglich zu machen. Sie muss aber sicherstellen, dass die angegebenen Tech-C und Admin-C über eine anonymisierte Email Adresse oder ein Webformular erreichbar sind (vgl. Ziffer 2.5.1 Temporäre Spezifikation).



Zudem muss die Antragsgegnerin die Daten gemäß Ziffer 4.1 der Temporären Spezifikation auf Anfrage an Dritte herausgeben, die ein berechtigtes Interesse an dem Zugriff darlegen können, es sei denn diese Interessen werden wiederum von den Interessen des Betroffenen überwogen. Damit sind die Voraussetzungen für die Offenlegung der Daten an die Voraussetzung des Art. 6 (1) f DSGVO geknüpft.

Eine solche Verpflichtung ist wesentlich, um berechnigte Interessen von einer breiten Gruppe von Personen zu schützen. Tech-C und Admin-C erfüllen wie dargelegt wichtige Funktionen bei der Unterstützung des Registrierenden in Bezug auf technische oder administrative Fragen und können rechtlich haftbar gemacht werden. Werden diese Daten nicht länger erhoben, ist eine solche Inanspruchnahme durch Strafverfolgungsbehörden und mögliche Anspruchssteller praktisch ausgeschlossen.

### III. Zuständigkeit des Landgerichts Bonn

Gemäß § 1033 ZPO ist das Landgericht Bonn international und örtlich zuständig, weil es – ohne die im RAA enthaltene Schiedsklausel – zuständig für einstweiligen Rechtsschutz wäre (Zöller/Geimer, § 1033, Rn. 3).

Artikel 5.8 des RAA enthält eine Schiedsklausel, wonach ein nach AAA Regeln zu konstituierendes Schiedsgericht zuständig wäre, mit Sitz in Los Angeles County, Kalifornien, USA. Jede der Parteien kann das schiedsgerichtliche Verfahren gegenüber dem gerichtlichen wählen. Allerdings schließt eine Schiedsklausel gemäß § 1033 nicht aus, dass die Antragstellerin am Sitz der Antragsgegnerin einstweiligen Rechtsschutz beantragt. Dies gilt auch, wenn der Sitz des potentiell in der Hauptsache zuständigen Schiedsgerichts im Ausland ist (OLG Köln, GRUR-RR 2002, 309; Zöller/Geimer, § 1033, Rn. 12 m. w. N.)

Schließlich heißt es in Artikel 5.8 RAA:

*Zur Unterstützung des Schiedsverfahren und/oder um die Rechte der Parteien während des Schiedsverfahrens zu wahren, haben die Parteien das Recht einstweiligen Rechtsschutz vom Schiedsgericht zu verlangen oder von einem Gericht in Los Angeles, Kalifornien, USA, was keinen Verzicht auf diese Schiedsklausel bedeutet.*

Erstens gilt diese Klausel ausweislich des Wortlauts nur während eines hängigen Schiedsverfahrens und zweitens ist die Zuständigkeit der amerikanischen Gerichte nicht ausschließliche. Zweitens, selbst wenn man davon ausgehen würde, dass diese Klausel auch vor Beginn eines Schiedsverfahrens und exklusiv gelten sollte, ändert das nicht an der Zuständigkeit des Landgerichts Bonn, weil diese Zuständigkeit für vorsorgliche Maßnahmen nicht derogiert werden kann (OLG Köln, GRUR-RR 2002, 309; OLG Frankfurt a.M., BeckRS 2013, 10147; Musielak/Voit, 15. Aufl. 2018, § 1033 Rn. 3 m.w.N.).

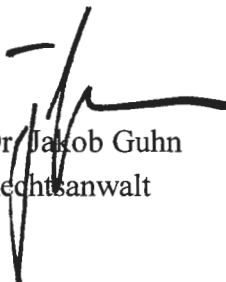
Im Leitsatz der Entscheidung des OLG Köln heißt es:

*Enthält eine Schiedsklausel die Vereinbarung, dass der vorläufige Rechtsschutz - soweit er durch staatliche Gerichte gewährleistet wird - ausschließlich dem zuständigen staatlichen Gericht am Sitz des Schiedsgerichts zugewiesen sein soll (hier: Stockholm), kommt einer solchen Regelung keine derogierende Wirkung zu. Für den vorläufigen Rechtsschutz ist - jedenfalls auch - das staatliche Gericht international und örtlich zuständig, das ohne die fragliche Schiedsklausel zuständig wäre (hier: Köln)*

Das OLG Köln begründet seine richtige Ansicht, dass eine Derogation der Zuständigkeit für einstweilige Maßnahmen ausgeschlossen ist, wie folgt:

*Diese Konsequenz [eine Derogation] widerspricht dem Grundgedanken des vorläufigen Rechtsschutzes, dem die Eilbedürftigkeit der jeweiligen Maßnahmen immanent ist. Den um Rechtsschutz Nachsuchenden in einer solchen Situation auf ein staatliches Gericht zu verweisen, welches unter Umständen ganz erheblich - womöglich tausende von Kilometern - vom Geschehen entfernt ist, würde einen effektiven vorläufigen Rechtsschutz in aller Regel ganz erheblich erschweren, wenn nicht sogar de facto ganz vereiteln, was den beiderseitigen Interessen der Parteien nicht entsprechen kann. (OLG Köln, GRUR-RR 2002, 309, 310)*

Diese Überlegungen sind vorliegend ebenso maßgeblich. Die Antragstellerin müsste ansonsten die einstweilige Verfügung vor amerikanischen Gerichten beantragen, welche dann im Rahmen des Eilrechtsschutzes über die Auslegung der europäischen Datenschutzgrundverordnung zu entscheiden hätten.



Dr. Jakob Guhn  
Rechtsanwalt