This English translation is provided for information purposes only. The official version of this document is available in German.

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

May 25, 2018

Via fax in advance (without appendices):0228 702-1600
Via courier
Regional Court of Bonn
Civil Chamber for Internet-related Disputes
Wilhelmstraße 21
53111 Bonn

DR. JAKOB GUHN
Office Düsseldorf
Assistant: Ms. Salowski
Phone 0211-5406-5532
Our reference: 530198-610043 JG

Motion for the issuance of a preliminary injunction

Internet Corporation for Assigned Names and Numbers (ICANN), represented by its president, Göran Marby, 12025 Waterfront Drive, Suite 300, Los Angeles, CA 90094-2536, USA,

- Applicant -

Attorneys of record: JONES DAY Rechtsanwälte,
Neuer Stahlhof, Breite Straße 69, 40213 Düsseldorf

versus

EPAG Domainservices GmbH, [redacted]

- Defendant -

<u>for:</u>	Cease and Desist, Contract, data collection and domain registration
<u>value in dispute:</u>	€ 1.000.000,00 (€ 1 Million)

May 25, 2018

We declare to be the attorneys of record of Applicant and ask the court:

> To order Defendant by way of a preliminary injunction, due to the urgency without prior oral hearing and issued by the presiding judge instead of the full bench, and under penalty of a disciplinary fine of up to EUR 250,000.00, to cease and desist,
>
> as an ICANN accredited registrar with regard to any generic Top Level Domain listed in Appendix AS 1,
>
> from offering and/or registering second level domain names without collecting the following data of the registrant that registers that second level domain name through the Defendant:
>
> > The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the registered second level domain names;
>
> and/or
>
> > The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the registered second level domain name.

REASONING

The Applicant is a non-profit public benefit corporation, which, among many other things, is responsible for contracting with entities to operate generic "Top Level Domains" and with entities that are responsible for registering second level domains within those Top Level Domains. A generic top level domain is the portion of a domain that is after the final dot, such as ".com" or ".org," as well as many others. A second level domain is the name just before the last dot, such as the "icann" in "icann.org."

The Applicant's mission is "[…] to ensure the stable and secure operation of the Internet's unique identifier systems […]". As one of the Applicant's primary roles is to be responsible for the Internet's identifiers, facilitating the ability to identify the holders of those identifiers is a core function of the Applicant.

The Applicant's mission to ensure the security and stability of the operation of the Internet's system of unique identifiers has led to the obligations associated with providing a "WHOIS" service. These obligations are contained in the Applicant's contracts and consensus policies (that are incorporated into contractual obligations) that the Applicant has with registries and registrars. These policies and contractual obligations govern the collection, retention, escrow, transfer, and display of WHOIS registration data, which includes contact information of natural and legal persons as well as technical information associated with a domain name registration. Through these policies and contracts, the Applicant sets the minimum requirements for WHOIS data, thereby ensuring the availability of WHOIS information to help mitigate attacks that threaten the stable and secure operation of the Internet and to serve other legitimate public interest uses.

Many registries and registrars are concerned about whether the Applicant's policies and contracts requiring them to collect, create, retain, escrow, and publish a variety of data elements related to registry/registrar operations, domain name registrations, and registrants are in conflict with the European Union's General Data Protection Regulation or "GDPR".

The Defendant is an "accredited registrar" of the Applicant. This means that the Defendant is authorized by contractual agreement with the Applicant to register second level domains within Top Level Domains allocated (through a separate contract) by the Applicant. As noted above, one of the Defendant's contractual obligations to the Applicant is to collect and retain certain required registration data from its customers.

The Defendant is now of the opinion that, as of 25 May 2018, because of the GDPR, the Defendant can no longer legally collect information on the technical contact and administrative contact as part of the customer data it gathers and is required to gather under its contract with the Applicant.

This view is incorrect. The technical contact and the administrative contact have important functions. Access to this data is required for the stable and secure operation of the domain name system, as well as a way to identify those customers that may be causing technical problems and legal issues with the domain names and/or their content. Therefore, GDPR provisions do not prevent the Defendant from collecting these data elements. If the Defendant does not collect the requisite technical contact or administrative contact information among other things, the secure operation of the domain name system and other legitimate uses of the data, such as law enforcement trying to locate bad actors that use the domain name system for criminal activity, will be in jeopardy.

Accordingly, the Applicant has attempted to convince the Defendant that it is still obligated under its contract with the Applicant to collect the administrative and technical contact information as part of the registration data it collects at registration. The parties were not able to solve this issue out of court. Therefore, the Applicant kindly asks the court to order the Defendant by way of preliminary ruling, not to sell respective new domain name registrations without collecting such data.

A. Facts

I. The Parties

The **Applicant** is a nonprofit public benefit corporation responsible for, among many other things, contracting with entities to operate generic Top Level Domains and with entities that are responsible for registering second level domains within those Top Level Domains. We submit a full list of the top level domains for which the Applicant contracts as

- Appendix AS 1 -.

The Applicant's mission is "[…] to ensure the stable and secure operation of the Internet's unique identifier systems […]". As one of the Applicant's primary roles is to be responsible for the Internet's identifiers, facilitating the ability to identify the holders of those identifiers is a core function of the Applicant.

As noted above, this mission has led to the obligations associated with providing a "WHOIS" service that are contained in Applicant's consensus policies and contracts that the Applicant has with registries and registrars, including the Defendant. These policies and contractual obligations govern the collection, retention, escrow, transfer, and display of WHOIS registration data for domain names in generic Top Level Domains, which includes contact information of natural and legal persons as well as administrative and technical information associated with a domain name registration. Through these policies and contracts, the Applicant sets the minimum requirements for WHOIS, thereby ensuring the availability of

WHOIS information to help mitigate attacks that threaten the stable and secure operation of the Internet.

We have attached excerpts from the website presence of the Applicant with a short explanation of the structure and tasks of the Applicant as

- Appendix AS 2-.

The **Defendant** is a German service provider in connection with the application and registration of domains in more than 900 Top Level Domains ranging from country code top level domains to new generic Top Level Domains. The Defendant also offers further services around registration of domains, as for example, domain backorders or management of a number of domain application procedures. We have attached excerpts from the website presence of the Defendant referring to their domain registration service as

- Appendix AS 3-.

II. The Registrar Accreditation Agreement between the Parties

The Applicant and the Defendant entered into a "Registrar Accreditation Agreement" signed on 22 January 2014 (hereinafter the "**RAA**"). We have attached the RAA and relevant passages translated into German as

- Appendix AS 4 -.

According to the RAA, the Defendant is "Accredited by ICANN to act as a registrar, including to insert and renew registration of Registered Names in the Registry Database". In other words: The Defendant is authorized by the Applicant to enter into domain registration agreements with customers wishing to get a second level domain within a Top Level Domain. As part of the registration process the Defendant was and is obliged to submit the data of the Name Holder to the Registry Operator maintaining the Registry Database for that specific Top Level Domain.

Section 3.4 stipulates that the relevant data shall be securely maintained by the Defendant in an electronic database. This obligation explicitly refers to the data listed in subsections 3.3.1.1 through 3.3.1.8 as follows:

> "*3.4.1 For each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain, in its own electronic database, as updated from time to time:*
> […]

3.4.1.2 The data elements listed in Subsections 3.3.1.1 through 3.3.1.8;"

Subsections 3.3.1.1 through 3.3.1.8 refer to the following data concerning all active Registered Names:

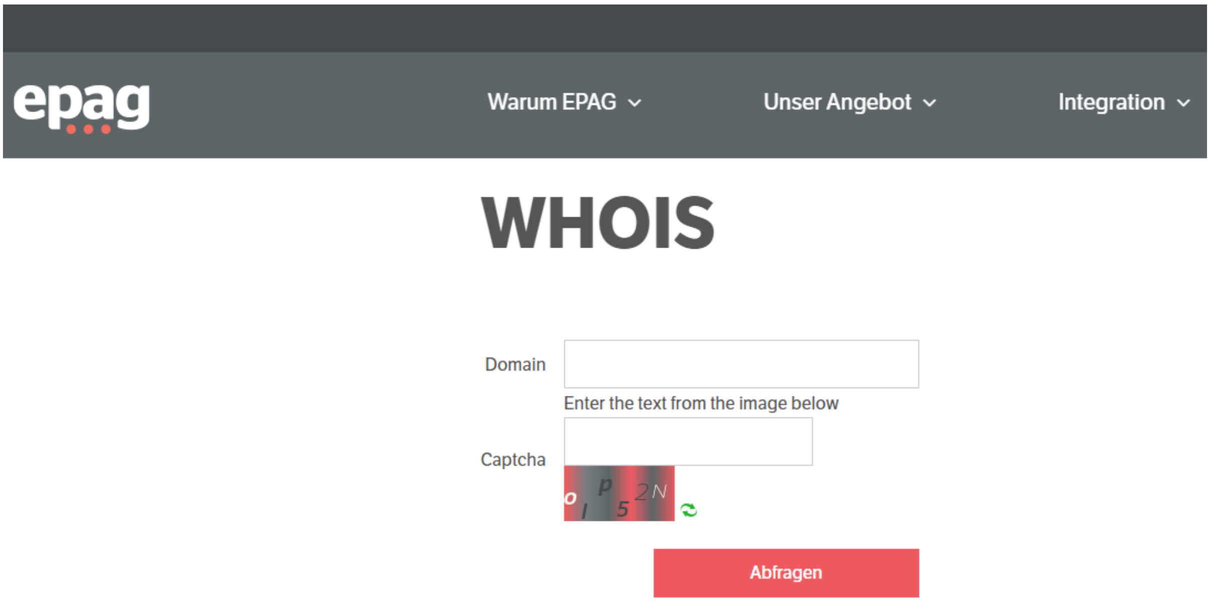
3.3.1.1 The name of the Registered Name;
3.3.1.2 The names of the primary nameserver and secondary nameserver(s) for the Registered Name;
3.3.1.3 The identity of Registrar (which may be provided through Registrar's website);
3.3.1.4 The original creation date of the registration;
3.3.1.5 The expiration date of the registration;
3.3.1.6 The name and postal address of the Registered Name Holder;
3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and
3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

On 17 May 2018, the Applicant's Board of Directors passed a "Temporary Specification," a single, unified interim model to ensure a common framework for registration data directory services, or "WHOIS" data, that would not violate the GDPR. The Temporary Specification did not change or alter, but rather reaffirmed the Defendant's requirements under the RAA as it relates to collection and retention of the data mentioned above. This is further explained below under section VIII 1.

III. The WHOIS System

These data points are fed into a data system with regard to the specific Top Level Domain within which a Second Level Domain name is registered. This data system is generally known as "WHOIS". WHOIS is not a centrally managed database. Rather, registration data is held in disparate locations and administered my multiple registries and registrars that set their own conventions for WHOIS service, consistent with the minimum requirements established in their agreements with the Applicant.

By way of reference we depict the WHOIS search interface provided by the Defendant available at www.epag.de/whois/ hereafter:



We have further enclosed excerpts from this search tool as well as a query for the Applicant's domain icann.org as

- Appendix AS 5 - .

WHOIS is a decentralized database that provides anyone, from law enforcement to anti-abuse volunteers to intellectual property interests to end users, with the ability to obtain contact information of individuals who have registered Internet resources such as domain names and internet protocol or "IP" addresses.

The service that the WHOIS system provides is essential, particularly for those involved in trademark matters, and those trying to combat fraud and abuse. The ability to obtain the WHOIS information is critical to helping to check availability of a domain name, and to track down persons participating in trademark infringement or abuse of those resources such as via phishing, spam, or fraud through misrepresentation of trademarks. The Applicant's mission to ensure the security and stability of the operation of the Internet's system of unique identifiers has led to the obligations associated with collection and retention of WHOIS data that are imposed on the parties with which ICANN has contracts.

The WHOIS system is vital for the management and security of the domain name system for several reasons including, but not limited to, the following:

1. Victim notification

When a website is compromised, or a previously legitimate mail server begins emitting spam, WHOIS information provides investigators and law enforcement officers with information to quickly contact the victim and assist in redress. WHOIS information is also used to notify organizations whose systems have been infected by viruses, especially ones that are infected, compromised and subsequently enrolled in "botnets" that are used for various nefarious purposes. In such cases of attack or abuse that threaten the stable and secure operation of the Internet, timely availability of contact information is often the first step to mitigate the attacks.

2. Attribution of criminal acts to a perpetrator

WHOIS data are critical information in online crime investigation. For instance, information found in the WHOIS system can be used as search terms within other databases, such as name server IP addresses in the domain name system, and email address databases maintained by anti-spam organizations, etc., which can assist law enforcement in obtaining a larger picture of the perpetrators activities. This aids law enforcement in both identifying the criminals as well as learning the scope of their activities.

3. Availability of a domain name

The WHOIS provides information on whether a certain domain name is already registered or not. Thus, market participants may check with WHOIS what domain name is still available and may become part of a new trademark strategy.

4. Enforcement of IP rights against Domain holder or participating persons

The ability to identify the holder of a domain name registration that is infringing a trademark is another use of the WHOIS system today. In some cases, trademarks that are used as domain names are registered in order to facilitate "phishing", or the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. In other cases, use of a trademark in a domain name is more benign - people either unknowingly or inappropriately registering another entity's trademark can cause confusion. In either case, being able to obtain the contact information associated with these domain names allows the intellectual property owners to engage with the people who have registered the domain name in order to address the infringement.

IV. Required Information for Domain registrations - Why the information is required for these purposes:

The data to be collected according to the Section 3.3.1.1-8 RAA refers to the relevant participants taking part in the registration and maintenance of the domain names and thus ensuring a stable and secure operation of domain name system.

The Defendant has questioned whether the data regarding the Technical Contact or **Tech-C** (3.3.1.7) and the Administrative Contact or **Admin-C** (3.3.1.8) are required for serving the purposes of the domain system mentioned above. The Defendant also has stated that it must not further collect data regarding the Tech-C and Admin-C because of GDPR provisions.

The data regarding the Tech-C and Admin-C, however, is essential part of the domain name system (see 1. and 2.). Further, the customer is not even required to provide personal data when referring to a Tech-C or Admin-C (see 3.).

In detail:

1. Tech-C – required data for the domain name system

The Tech-C is the relevant contact person in case of technical issues with a domain name.

The position of a Tech-C was created in order to make sure that all domain name registrants identify a person, entity or "roll account" with just a title, where a party can go to find a party with the technical skills to solve technical issues with the domain name in question. Further, this position was created in order to give the domain name registrant the possibility to delegate this position to another person being a) the IT-expert within the registrant firm, or b) a service provider specialized on such technical service.

Thus, in practice the Tech-C has access to the domain and is responsible for solving any technical issue with regard to the domain name on behalf of the registrant.

This Tech-C position thus facilitates the solution of technical issues. For example, where the domain name registrant is a legal person and no different information for Tech-C is given, the person to be contacted in case of issues would be an identified representative. In particular in larger corporations, this may significantly delay resolutions of technical issues if the CEO or other member of the management that it identifies as the representative of the legal person has to be contacted first in order to resolve the technical issue. Also where the registrant is a natural person it may be beneficial to entrust a third person with the Tech-C role, for example where the registrant is inexperienced in technical matters.

The RAA requires the registrar to collect the following data for the Tech-C:

- name,
- postal address,
- e-mail address,
- voice telephone number,
- and (where available) fax number

Such data is necessary to identify the Tech-C and to have appropriate means to contact the Tech-C. In particular an e-mail address and a voice telephone number are required. There are a multitude of reasons why swift contact with the Tech-C may be required. For example, when a webserver that is connected to a specific domain was subject to a cyber-attack and the attackers have infected the webserver with malicious code that now infects visitors of that domain, time is of the essence. Relying on communication via post or even e-mail may be too slow to prevent further harm to a great number of Internet users.

2. Admin-C – required data for domain name system

The Admin-C is the person or entity entrusted with the administrative control of the domain name with the right to access the domain name, to change its contact or even to transfer the domain name registration to another registrar or registrant. Thus, the Admin-C is the person fully authorized and responsible person for name registration dealing with all administrative or legal issues with the domain. The ability to name an Admin-C provides an important and legitimate option for the domain name registrant to delegate the obligations in connection with the registration and use of a domain to a competent person within or outside its firm.

The domain name registrant may not always be the most suitable person to deal with the day-to-day business of a domain name. While it may elect to serve as the Admin-C itself, the registrant may also delegate that function to a more suitable person.

This position and respective tasks are not only common practice and the allocation of responsibilities and liabilities has been acknowledged by German courts. The German courts consider the Admin-C as the "facility manager" of the domain who has to make sure that any legitimate request to delete infringing content from the domain website is followed by the Admin-C (st. Rspr. BGH GRUR 2012, 304 – Störerhaftung des Admin-C bei Verletzung besonderer Prüfpflichten; OLG München BeckRS 9989, 52174 - *intershopping.com*). The Admin-C is also responsible and possibly liable for legitimate use of the domain.

The need to be represented by an Admin-C becomes even more obvious when looking at the number of generic Top Level Domains and respective legal provisions to be regarded. If the availability of designating an Admin-C is removed, as the Defendant suggests is necessary for data protection reasons, the domain name registrant would not have the option to delegate this task anymore. He could only transfer registration of the domain name in order to be able to delegate responsibilities, for example by way of an escrow agreement.

As a result, the publication that the domain name registrant has delegated Admin-C tasks to a certain person is important information for any third party dealing with that domain name or the content displayed on its website. Therefore, there should not be any doubt that the Admin-C function and the respective collection of data of those serving in that role is based on legitimate reasons.

This result is also supported by a comparative view on the trademark registers worldwide. The European trademark register, for example, enables each trademark owner to name a legal representative taking care of all communication and applications. The aim is that each trademark owner is supported by a specialist who is aware of the obligations to be fulfilled under European trademark law. The European trademark register (EUIPO) and third parties may serve documents with such specialist. Thus, the legal representative, as well as the Admin-C, ensure proper functioning of the respective system.

3. What data is collected regarding the Tech-C and Admin-C?

When assessing the legality of collecting and processing the data for the Tech-C and Admin-C, namely name, postal address, e-mail address, voice telephone number, and (where available) fax number, also the following must be considered:

(1) There is no obligation that the Tech-C is a natural person. Instead it may be a legal person or a roll account with just a title; and

(2) The Tech-C may also be the same natural or legal person than the registrant.

Where the data for the Tech-C constitutes personal data (and therefore is subject to the GDPR), there are two possible categories of data

(*i.*) the data is identical to the registrant, and (*ii.*) the data differs from the data collected from the registrant.

In the **first scenario** no "new" data is collected. If no Tech-C data were collected, any requests regarding technical issues were to be directed to the domain registrant, i.e., in case of a legal person to the legal representatives. Thus, such collection does not lead to a collection of further personal data.

In the **second scenario**, where the registrant chooses to name a person other than itself, and in case such data constitutes personal data, the collection of such data is subject to an assessment under the GDPR and will be evaluated in the legal reasoning below. But the answer to this question is that the GDPR does not have the aim to not further collection of contact data which are essential part of an important infrastructure system and which serves legitimate and important purposes.

V. Comparison between WHOIS system and trademark register

These functions and contents of such a domain data system or WHOIS system compare well with a trademark register whereby the domain system is Internet-related only leading to further challenges:

1. Trademark registers

With the international treaty on "Trade-Related Aspects of Intellectual Property Rights" (TRIPS) all relevant economies of the world have agreed on a certain level of protection regarding several intellectual property rights, including trademarks. As a consequence, each trademark system based on these TRIPS rules has its own trademark register collecting all required data as follows:

a. Content of a trademark register

The European Trademark Register shows all relevant data regarding a registered European Trademark, including but not limited to personal data of the owner and a (required) legal representative representing the trademark owner, including all contact details (address, telephone number, facsimile number and email) as well as all correspondence and legal decisions in connection with this trademark application.

By way of an example, we have attached a full copy of a trademark registration EUTM 002886448 DOPODOPO and respective information as

- Appendix AS 6 - .

Comparing this content with the WHOIS system, basically the same data are collected from the trademark owner and the domain name registrant whereby a) the trademark owner usually refers to a legal representative dealing with communication and legal issues, and b) the domain name registrant may refer to a Tech-C and an Admin-C dealing with technical and legal issues regarding the domain.

b. Functions of Trademark register

The trademark register referring to basically the same data has basically the same functions as WHOIS:

i. Law enforcement – victim notification and attribution to criminal acts

The trademark register helps public authorities, for example during investigations on sale of counterfeits. The trademark register shows the legitimate trademark owner and makes it easier to identify and contact suspects or parties concerned by fraud or trademark infringement.

This function compares well with WHOIS system where victims of internet fraud may be identified via WHOIS and informed immediately.

ii. Availability of a trademark

Both trademark registries and the WHOIS system enable market participants to check availability of a certain sign or name to be used in the future. And market participants interested in a certain trademark or domain name may check the existence of the registration and participating parties.

iii. Enforcement of trademark rights

The trademark register has also the important public function to enable market surveillance. The courts also require trademark owners to conduct market surveillance in order not to lose their right to enforce its trademark (see BGH GRUR 2016, 705, 709). And the trademark owners need to be able to further investigate existence of other trademark rights in the market in order to evaluate the chances and risks of trademark infringement.

The WHOIS systems serves basically the same purpose whereby the scope of data and information of the trademark register is much broader than within the WHOIS system for domain names.

2. Trademarks and domain names

As said before, trademarks and domain names generally have a similar function, which is to distinguish offers for goods and services in a market.

The legal basis of trademarks and domain name, however, differs. Trademarks are constitutional part of each law regime subject to the TRIPS treaty. As a consequence, the signatories to that treaty have implemented trademark laws with explicit rules regarding the procedures and the stable and secure maintenance of a trademark register.

With regard to domain names, however, the situation differs. The domain name system or **"DNS"** is a decentralized naming system for computers, services, or other resources connected to the Internet. The existence and maintenance of the DNS is not based on international treaties between all participating member states. It is based on contractual agreements between the parties involved. Thus, there is no law in place regulating the collection of data regarding domain names in detail.

Nevertheless, the need for existence and functions of the DNS is without question. And the courts need to find their ways to attribute required rights and obligations surrounding the DNS by interpretation of the law, by analogous application of law or by development of the law.

VI. The implementation of the GDPR

On 14 April 2016, the European Union (EU) adopted the General Data Protection Regulation (GDPR), which takes effect on 25 May 2018. In Germany it supersedes the BDSG. According to the European Commission, the aim of the GDPR is to protect all EU citizens and residents from privacy and data breaches. It applies to all companies processing and holding the personal data of subjects residing in the European Union.

The GDPR only allows collection and processing of personal data for specific purposes (Art. 5(1) lit. b GDPR), which need to be set out by the entity or person controlling the data. Without giving a particular purpose for the collection and processing of data, any such actions will be unlawful. Additionally, Art. 5 GDPR sets out other requirements for the processing to be lawful (e.g., good faith in Art. 5 (1) lit. a and data minimization in Art. 5 (1) lit. c GDPR).

The legitimate purpose is also the guiding principle when determining which data may be processed with a view on the data minimization (Ehmann/Selmayr, Art. 5 Rn. 13). If processing is necessary to meet the legitimate purpose this step will be lawful under the GDPR. The purpose needs to be clear in order for the data subject to be informed why the data is processed (see also Art. 13 and 14 GDPR which govern the questions of what information must be provided to the data subjects when processing the data).

Furthermore, Art. 6 GDPR explains in which circumstances a collection and processing is allowed which include *inter alia* consent of the data subject (Art. 6 (1) lit. a GDPR), necessity for the performance of a contract (Art. 6 (1) lit. b GDPR), necessity to fulfil other legal requirements but a contract (Art. 6 (1) lit.c GDPR), and – importantly – legitimate interest in the processing if the rights of the data subject do not outweigh these interests (Art. 6(1) lit. f GDPR). The weighing of the interests has to be performed by the controller of the data at its own accord (Ehmann/Selmayr, Art. 6 Rn. 27).

VII. No Impact of GDPR on trademark registers

The implementation of the GDPR on 25 May 2018 has no influence whatsoever on the collection and publication of personal data in trademark registries. All the data mentioned above are further collected and made publicly available to people inside and outside the European Union. The reason for that is quite simple. The law regimes have implemented legal provisions that foresee the collection and publication of relevant data. These legal provisions imply the necessity of collection of data. Therefore, the GDPR does not question legacy of such data collection.

VIII. Impact of GDPR on WHOIS system

With regard to the WHOIS system, however, many experts in the domain name industry shared their opinion that the implementation of GDPR has to lead to significant changes regarding the collection and maintenance of data in connection with domain name registrations. Their argument is basically that certain data collected within the WHOIS data base are not necessary to meet a legitimate purpose. Such reservations are predominantly directed against how and to whom such data is disclosed.

1. Implementation of Temporary Specification by ICANN

The GDPR has given prominence and urgency to the debate about data protection and privacy in the WHOIS ssytem. The Applicant took the concerns mentioned above very seriously. Over the past several months the Applicant has consulted with community stakeholders, contracted parties, European data protection authorities, legal experts, and interested governments to understand the potential impact of the GDPR to personal data that participants in the gTLD domain name ecosystem collect, display and process (including registries and registrars) pursuant to the Applicant's contracts and policies. As a result, the Applicant has adopted a Temporary Specification on the collection and use of data within the WHOIS system. We have attached a copy of the Temporary Specification provisions as

-Appendix AS 7-.

When the Temporary Specification goes into effect on 25 May 2018, the WHOIS system will remain available, though there will be some changes. Importantly, registry operators and registrars are still required to collect all registration data, which is consistent with the Applicant's stated objective to comply with the GDPR, while maintaining the existing WHOIS system to the greatest extent possible.

The Temporary Specification binds all registrars, including the Defendant, as per section 4 of the RAA and the "Consensus Policies and Temporary Policies Specifications".

The Temporary Specification describes in section 4.4 the purposes for which the data is collected and processssed. *Inter alia,* the rights of the registrant or "Registered Name Holder" are reflected (section 4.4.1). Furthermore, processing may occur for purposes of providing access to accurate, reliable and uniform registration data based on legitimate interests not outweighed by fundamental rights of the data subjects (section 4.4.2), including for the purpose of enabling technical and administrative points of contact adminiserting the domain names at the request of the registrant (section 4.4.7).

The Temporary Specification further sets out why the Applicant has come to the conclusion that collection and processing of the data is proportionate (section 4.5). It also sets out what the Registrar has to notify to existing and new Registered Name Holders (section 7.1, which replaces section 3.7.7.4 of the RAA).

If Internet users submit a WHOIS query, at a minimum the user will still receive some or "thin" data in return, including technical data sufficient to identify the sponsoring registrar, status of the registration, and creation and expiration dates for each registration. Additionally, the user will have access to an anonymized email address or a web form to facilitate email communication with the relevant contact (e.g., registrant, administrative, technical contacts). The Applicant is expected to enforce the Temporary Specification as it is fully incorporated into the relevant registry agreements and registrar accreditation agreements.

2. Obligations of Registrars under Temporary Specification

As a consequence, the Applicant has taken care of the implementation of GDPR and its impact on the WHOIS system. At the same time, however, the registrars are still obliged to collect and provide the required data mentioned in the RAA (as confirmed by the Temporary Specification).

In particular, the Defendant is obliged to collect and to keep the data on the Tech-C and the Admin-C.

IX. Legal position of the Defendant

The Defendant has expressed its opinion that it should not collect data with regard to the Tech-C and the Admin-C because the Defendant thinks doing so violates the GDRP.

The Parties discussed these issues in several calls. And the Applicant raised its concern and explicitly mentioned that the Applicant is ready to file preliminary injunction proceedings in Germany in order to obtain a judgment of a German court in this matter.

Further, on **24 May 2018**, the Parties had a conference call with the following participants:

[redacted], John Jeffrey, General Counsel and Secretary of the Applicant, Amy Stathos, Deputy General Counsel ICANN, Erika Randall, Associate General Counsel of the Applicant [redacted]

The signatory Jakob Guhn summarized the situation and concerns of the Applicant and kindly asked the legal representative of the Defendant to explain its legal position regarding the announced non-collection of data as of 25 May 2018.

[redacted] confirmed in response that as of 25 May 2018 the Defendant will not further collect Admin-C and Tech-C data from registrants.

Furthermore, [redacted] stated that as of 25 May 2018, the customers of the Defendant will be in the position to delete the data regarding the Tech-C and Admin-C with regard to registered domains. In addition, during this call, the Defendant stated that it was working on a plan for systematic deletion of such data but this plan is not implemented yet, but that is no longer the case as confirmed by John Jeffrey as indicated below.

The content of this call is **legally assured** by the signatory Jakob Guhn.

In a follow up call on the same day between [redacted] and John Jeffrey, [redacted] agreed that EPAG will not permanently delete WHOIS data collected, except consistent with ICANN's policy, and if that changed he would notify ICANN before taking any such action. On the other hand he confirmed that the Defendant will only collect registrant data – not Admin-C data and Tech-C data.

We submit a respective affidavit signed by John Jeffrey as

-Appendix AS 8-.

Further, [redacted] announced that he would send a letter to the Applicant explaining the Defendant's standpoint more in detail. So far, the Applicant has only received a "DRAFT" letter. As soon as the Applicant receives a binding statement of the mother company of the Defendant, however, we will forward such letter to the court.

As a consequence, there is a high risk that – as of 25 May 2018 – the Defendant will no longer collect and maintain the following data, explicitly mentioned in 3.3.1.7 and 3.3.1.8 in the RAA and approved by Temporary Specifications:

> The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name;

and

> The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

B. Legal Assessment

The application for injunctive relief is well-founded. The Applicant has a claim for cease and desist (below I) as well as it is able to rely on urgency as a reason for injunctive relief because the Defendant announced that it would stop collecting Admin-C and Tech-C data as of 25 May 2018 (below II).

I. Claim for injunctive relief

The Applicant has a contractual claim against the Defendant to only offer and sell domain names when the data specified in the claim for injunctive relief are collected and maintained.

The Applicant has a contractual claim against the Defendant to process the data as agreed in section 3.3.1.1 to 3.3.1.8 RAA, including the data with regard to the Tech-C (3.3.1.7) and the Admin-C (3.3.1.8). The Applicant has a further claim according to Section 3.4.1.2 that the Defendant securely maintains this data. This obligation refers to each registered domain name sponsored by the Defendant, i. e., having placed the record associated with that registration into a registry, 1.26 RAA.

In spite of this contractual claim, the Defendant has threatened not to collect data regarding Tech-C and Admin-C of new domain registrations beginning immediately. Further, the Defendant may be working on a plan to permanently delete Admin-C and Tech-C data in the near future. The alleged reason for this non-collection and possible deletion is the coming into force of the GDPR. However, the GDPR does not change the contractual obligations of the Defendant – it is still obliged to collect and to keep the data under Art. 6 (1) lit. a and/or f GDPR.

The only data elements in dispute are the Tech-C and Admin-C details as for the other ones the Defendant seems to acknowledge its duty to further collect and maintain. Boat of these data sets should be collected for the following reasons:

1. No personal Tech-C or Admin-C data – no applicability of GDPR

As mentioned above, many Tech-C and Admin-C data do not even refer to personal data. The GDPR is, however aimed

> *“on the protection of* ***natural*** *persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)” (Subtitle of the GDPR Regulation).*

Therefore, the Defendant tries to justify non-collection of this data without looking into detail whether the concrete data referring to the Tech-C or Admin-C constitutes personal data.

2. Art. 6 (1) (a) GDPR

In case Tech-C or Admin-C data constitutes personal data the collection of the data is permissible, in particular, on the basis of consent of the data subject pursuant to Art. 6(1)(a) GDPR.

Art. 6(1)(a) GDPR says that processing shall be lawful if and to the extent that:

> *"(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;"*

In fact, under the RAA (including the Temporary Specification), the Defendant is not hindered to seek consent from the Tech-C or Admin-C to acquire their data. To the contrary, section 7.2 of the Temporary Specification specifically provides that:

> "*7.2.2. Registrar MAY provide the opportunity for the Admin/Tech and/or other contacts to provide Consent to publish additional contact information outlined in Section 2.4 of Appendix A.*"

While it remains unclear, why the Defendant does not explore such option, the Defendant cannot argue that consent of the Tech-C and Admin-C would be void pursuant to Art. 7 GDPR. In particular, there is no violation of Art. 7 (4) GDPR:

> *(4) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

The performance of the domain name registration is not conditional on the provision of consent. Where the person designated by the customer to act as Admin-C or Tech-C does not consent, the role of the Admin-C / Tech-C will remain with the Registrant. Under the RAA (including the Temporary Specification), there is no obligation that the Tech-C and/or Admin-C must be identified using personal data or be a person different than the registrant. Thus, the domain name applicant may register the domain name without providing personal data at all.

3. Art. 6 (1) lit. b GDPR

According to Art. 6 (1) lit. b) GDPR processing shall be also lawful if and to the extent that:

> *(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

Also these requirements are fulfilled in the present case.

The position of the Admin-C and Tech-C is an important option for the registrant to delegate tasks regarding its registered domain names. And, according to the RAA the Defendant has to collect such data with regard to any new domain name registration. The failure of the Defendant to collect (or potential delete in the future) the reference to the Admin-C and Tech-C would make it impossible for the registrant to benefit from this option.

Thus, there should not be any doubt about the question that the collection of such data is required for the performance of the contract.

4. Art. 6 (1) lit. f GDPR

In addition to this, it is in the legitimate interest of the public to maintain the data the Defendant previously collected (Art. 6 (1) lit. f GDPR). According to Art. 6 (1) f) GDPR processing shall be lawful if and to the extent that

> *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

The Applicant has explained in detail the important option for the registrant to delegate tasks regarding its domain to a Tech-C or to an Admin-C. These functions are an essential part of the domain name system making sure that also large companies and natural persons without having a technical background are in the position to name an individual, through name or title, or a professional service provider, as such contact. The use of personal data of a natural person is not required. And – if any personal data is provided – such data is often restricted to mere contact details within the firm.

The comparison to trademark data bases also show that such legitimate interest for the collection of such data should be out of question. Trademark databases collect comparable data in order to give the opportunity to delegate tasks with regard to the registration and maintenance of the trademark to a legal representative being the expert to trademark matters. Thus, basically the same data is collected for the same functions and aims mentioned above. And it is not even discussed whether such collection of data should trigger data protection concerns.

The Applicant has also explained in detail the purpose of collecting such data as set out in section 4.1 – 4.3 of the Temporary Specification:

> *ICANN's mission, as set forth in Bylaws Section 1.1(a), is to "coordinate the stable operation of the Internet's unique identifier systems." Section 1.1(a) describes in specificity what this mission entails in the context of names. While ICANN's role is narrow, it is not limited to technical stability. Specifically, the Bylaws provide that ICANN's purpose is to coordinate the bottom-up, multistakeholder development and implementation of policies "[f]or which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability*

> *of the DNS including, with respect to gTLD registrars and registries" [Bylaws, Section 1.1(a)(i)], which is further defined in Annex G-1 and G-2 of the Bylaws to include, among other things:*
>
> *• resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names);*
>
> *• maintenance of and access to accurate and up-to-date information concerning registered names and name servers;*
>
> *• procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar (e.g., escrow); and*
>
> *• the transfer of registration data upon a change in registrar sponsoring one or more registered names.*
>
> *The Bylaws articulate that issues surrounding the provision of Registration Data Directory Services (RDDS) by Registry Operators and Registrars are firmly within ICANN's mission. The Bylaws provide further insight into the legitimate interests designed to be served by RDDS. For example, the Bylaws specifically obligate ICANN, in carrying out its mandate, to "adequately address issues of competition, consumer protection, security, stability and resiliency, malicious abuse issues, sovereignty concerns, and rights protection" [Bylaws Section 4.6 (d)]. While ICANN has neither the authority nor expertise to enforce competition or consumer protection laws, and is only one of many stakeholders in the cybersecurity ecosystem, the provision of RDDS for legitimate and proportionate uses is a critical and fundamental way in which ICANN addresses consumer protection, malicious abuse issues, sovereignty concerns, and rights protection – enforcing policies that enable consumers, rights holders, law enforcement and other stakeholders to access the data necessary to address and resolve uses that violate law or rights.*
>
> *Accordingly, ICANN's mission directly involves facilitation of third party Processing for legitimate and proportionate purposes related to law enforcement, competition, consumer protection, trust, security, stability, resiliency, malicious abuse, sovereignty, and rights protection. ICANN is required by Section 4.6(e) of the Bylaws, subject to applicable laws, to "use commercially reasonable efforts to enforce its policies relating to registration directory services," including by working with stakeholders to "explore structural changes to improve accuracy and access to generic top-level domain registration data," "as well as consider[ing] safeguards for protecting such data." As a result, ICANN is of the view that the collection of Personal Data (one of the elements of Processing) is specifically mandated by the Bylaws.*

Thus, the Applicant has clearly set out why the interests of the public outweigh any interest of the data subject when processing Tech-C or Admin-C details.

Balancing these interests, there is no doubt that collection of such data is justified under GDPR. Thus, the Defendant may not argue that GDPR hinders the Defendant from fulfillment of its contractual duties under the RAA.

II. Reason for injunctive relief

The matter is urgent. The Applicant has taken immediate steps when it first learned that the Defendant will not comply with its contractual obligations to collect the data in question going forward. Injunctive relief is also necessary to prevent irreparable harm. With this application, the Applicant seeks to ensure that all WHOIS data elements are collected.
On or about May 14, 2018, the Applicant, in person of John Jeffrey, General Counsel and Secretary of the Applicant, first learned from [redacted] the mother company of the Defendant, that the Defendant may not continue to collect certain data regarding domain registrations as of 25 May 2018.

In a statement of 17 May 2018, inter alia Tucows Inc., requested a moratorium for implementing the Temporary Specification, "*providing us an opportunity to conform, to the extent possible, our GDPR implementation with the GDPR-compliant aspects of any ICANN temporary specification.*"

Then, in two further calls on 24 May 2018, the Applicant was more specifically informed about the concrete plans of the Defendant as outlined above. Thus, the matter is urgent.

The Defendant's non-compliance with its contractual obligations will cause irreparable harm. Once, the Defendant does not collect the data of Admin-C and Tech-C this data is lost. To account for uncertainties regarding the current WHOIS system, the Applicant has passed the Temporary Specification for gTLD Registration Data. Under the Temporary Specification, while the Defendant is under no obligation to publicly disclose the Admin-C and Tech-C data, it must enable contact with the Admin-C and Tech-C via an e-mail address or web form, which must not identify the contact e-mail address or the contact itself, Sec. 2.5.1 Temporary Specification.

In addition to that, pursuant to section 4.1 of the Temporary Specification, the Defendant must make the data of the Admin-C and Tech-C available to a third party based upon legitimate interest unless where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6 (1) (f) GDPR. Thus, the requirements to disclose such data is aligned with the requirements to justify such processing under Article 6 (1) (f) GDPR.

Such obligation is vital to protect the legitimate interests of a wide group of people. As explained above, the Tech-C and Admin-C have crucial roles in supporting the registrant with technical issues and administrative issues and can be held legally accountable. Where such data is not collected, holding the Tech-C and Admin-C accountable by law enforcement agencies and potential claimants will be practically impossible.

III. Competence of the Court

Pursuant to Section 1033 of the German Code of Civil Procedure (Zivilprozessordnung, ZPO), the Regional Court of Bonn is the locally competent court because it would be competent to grant injunctive relief, but for the arbitration agreement in the RAA (Zöller/Geimer, § 1033, Rn. 3).

The RAA in section 5.8 contains an arbitration agreement providing for AAA arbitration in Los Angeles County, California, USA. Either party may chose arbitration over litigation. An arbitration agreement, however, does not exclude Applicant from requesting injunctive relief at Defendant's registered seat as per Section 1033 ZPO. This is equally true if the seat of the arbitration is agreed to be outside Germany (OLG Köln, GRUR-RR 2002, 309; Zöller/Geimer, § 1033, Rn. 12 m. w. N.).
Finally, the parties agreed in section 5.8 RAA *in fine* that

> *"For the purpose of aiding the arbitration and/or preserving the rights of the parties during the pendency of an arbitration, the parties shall have the right to seek temporary or preliminary injunctive relief from the arbitration panel or in a court located in Los Angeles California, USA, which shall not be a waiver of this arbitration agreement."*

First, this provision only relates to injunctive relief during a pending arbitration and is non-exclusive.

Second, even if it were to apply also prior to an arbitration and exclusively, this agreement would not derogate this court's competence to grant injunctive relief (OLG Köln, GRUR-RR 2002, 309; OLG Frankfurt a.M., BeckRS 2013, 10147; Musielak/Voit, 15. Aufl. 2018, § 1033 Rn. 3 m.w.N.).

In the lead sentence of the OLG Cologne it is held:

> *If an arbitration agreement encompasses an agreement that interim relief – as far as to be granted by state courts – may exclusively be granted by the competent court at the seat of the arbitration (here: Stockholm), such agreement does not have derogative effect. For interim relief the state courts which would be competent failing the arbitration agreement are – at least also – internationally and locally competent (here: Cologne).*

The OLG Cologne bases the correct reasoning that a derogation of interim relief competence is excluded on the following considerations:

> *This consequence [a derogation] is contrary to the underlying reasoning for interim relief, which encompasses the urgency of the respective measure. To refer the person seeking legal protection in such situation to a state court which can be very far away from the events – potentially thousands of kilometers – would as a rule significantly complicate effective interim relief, if not de facto exclude it, which cannot be in the interests of the parties."*

OLG Köln, GRUR-RR 2002, 309, 310

These considerations apply here as well. The Applicant would have to request interim relief before US state courts which would then have to decide in the ambit of an interim relief request on the interpretation of the European GDPR.

Dr. Jakob Guhn
Attorney-At-Law