

JONES DAY

RECHTSANWÄLTE • ATTORNEYS-AT-LAW • PATENTANWÄLTE
NEUER STAHLHOF • BREITE STRASSE 69 • D-40213 DÜSSELDORF
TELEFON: +49.211.54065.500 • TELEFAX: +49.211.54065.501

June 13, 2018

Via fax in advance: 0228 702-1600

Via courier

Regional Court of Bonn
10th Civil Chamber
Wilhelmstraße 21
53111 Bonn

DR. JAKOB GUHN
Büro Düsseldorf
Sekretariat: Frau Salowski
Tel. 0211-5406-5532
Unser Zeichen: 172210-690003 JG

Immediate Appeal

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 -

Attorneys of record: Rickert Rechtsanwaltsgesellschaft mbH
Kaiserplatz 7-9, 53113 Bonn

Docket- No.: LG Bonn 10 O 171/18

We hereby submit an immediate appeal on behalf of the Applicant and **ask the court:**

To lift the decision of the Regional Court of Bonn of 30 May 2018, docket-no. 10 O 171/18

and

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,

1. 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 a 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.

And in the **alternative**,

2. 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 a second level domain name through the Defendant,

- a) whereby the data is provided with requested consent of the persons named regarding use of the personal data,

and/or,

- b) whereby the data does not contain personal data relating to a natural person,

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 preliminary ruling of May 29, 2018, docket no 10 O 171/18 (hereinafter the “**Decision**”) of the Chamber is not consistent with the facts at hand. Further, the decision is not tenable.

In its order the Chamber would not require the Defendant to fulfill its contractual obligation to collect data referring to the administrative contact (“**Admin-C**”) and the technical contact (“**Tech-C**”) data when it accepts a domain name registration.

The Chamber has based its decision on the universal legal principle that a party may only demand performance of contractual obligations to the extent such performance does not violate any applicable laws (p. 7 of the judgment). While this principle is not disputed, Defendant could only refuse performance of its obligations under the aforementioned principle if there was **no lawful way** to fulfill such obligation. However, this is not the case. There are several lawful ways to fulfill such obligations, in particular:

1. by collecting data elements for the Admin-C and Tech-C that do not constitute personal data; or
2. by collecting data elements for the Admin-C and Tech-C that do constitute personal data, but where processing is justified based on:
 - a) consent of the data subject, Art. 6 (1) a) GDPR;
 - b) necessity for performance of the contract, Art. 6 (1) b) GDPR; or
 - c) legitimate interests, Art. 6 (1) f) GDPR.

Neither the Registrar Accreditation Agreement (RAA) Defendant has entered with the Applicant, nor the Temporary Specification that amends the RAA in some ways, requires Defendant to collect Admin-C and Tech-C data in a specific way. Accordingly, the Defendant is free to choose a manner to collect Admin-C and Tech-C data that is **indisputably** compliant with the GDPR in order to fully comply with its obligation.

Even the Chamber apparently acknowledges that there is a legitimate way to collect the Admin-C and Tech-C data assuming that the Defendant collects such data that is provided by the registrant of her own free will and with respective consent (page 7 of the Decision). However, **the Defendant does not collect the Admin-C and Tech-C data in any case**, (a) no matter whether the data constitute personal data or not, and (b) no matter whether this data was provided with consent or not. This is a clear breach of the Defendant’s contractual obligation, which is not justified by GDPR provisions.

A. FACTS

The Applicant needs to stress again certain facts in order to make sure that the Chamber duly evaluates the restricted impact of GDPR to contractual obligations of the Defendant:

The Defendant has decided not to collect any Admin-C or Tech-C data at all, no matter whether the GDPR provisions apply and no matter whether the subject has provided consent (see I.). A legitimate purpose of the Applicant is to offer the option for the registrant to delegate administrative and technical tasks to a third person. At the same time, such collection of Admin-C and Tech-C data serves the objectives of, among other things, law enforcement, child protection, consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection (see II.). These legitimate purposes are specified and explicitly mentioned below (see III.). The data to be collected for Admin-C and Tech-C *may be* personal data if the registrant wishes to do that. If the registrant does provide personal data, the collection of such personal data is also necessary (see IV.). The Defendant is also not hindered to collect explicit consent of the Admin-C and Tech-C. To the contrary, the Defendant is obliged by contract to collect consent of all relevant data subjects (see V.). As a consequence, the Defendant must also collect such data in order to ensure contractual fulfillment (see VI.). It is also without question that all participants have a legitimate interest to use personal data if the data subject has provided such data on its own free will, because it wishes to be contacted in certain cases (see VII). Finally, the Admin-C and Tech-Data will in any case not be published in the WHOIS system without explicit consent (VIII).

In detail:

I. The Defendant no longer collects data no matter whether GDPR applies

The Chamber appears to be under the impression that the registrant may still designate an Admin-C and a Tech-C upon consent of the data subject. However, as of 25 May 2018, the Defendant made clear that this is not the case anymore within the Defendant's systems. The Defendant has indicated that it will "no longer collect the data for the Admin-C and Tech-C," (protective letter, p. 5) which deprives all registrants of the option to name an administrative and technical contact:

1. The Chamber's assumption – Registrants may still provide Admin-C and Tech-C voluntarily?

In the reasoning of the Decision, the Chamber stresses its opinion that a registrant still can provide details for the Tech-C and the Admin-C with the Tech-C's and the Admin-C's consent:

“[...] *So far as the choice to provide contact data for Admin-C and Tech-C was with the registrant in the past [...] it means that the person wishing to register **will also be able to voluntarily provide corresponding personal data in the future in case of consent to the collection and storage thereof** (Art. 6 (1) a) GDPR and para. 7.2.2 of the RAA) [...]*” (Emphasis added, page 7 of the Decision)

2. The Defendant no longer collects Admin-C and Tech-C data

In its protective letter the Defendant has confirmed that it will not collect any Admin-C and Tech-C data. That announcement **is not subject to any qualifications** such as that it would not collect Admin-C and Tech-C data in case it constituted personal data and no consent was provided. To the contrary, pursuant to its announcement, the Defendant will not collect Admin-C and Tech-C data under any circumstances:

“The Defendant has stated that it will no longer collect the data for the Admin-C and the Tech-C, [...]” (protective letter, p. 5)

“Die Antragsgegnerin hat verlauten lassen, dass sie die Daten für den Admin-C und den Tech-C nicht weiter erheben wird, [...]” (Schutzschrift, S. 5)

Thus, in the light of this Defendant’s announcement, it will not be possible to voluntarily provide Admin-C and Tech-C data even if consent was provided.

The reason for not asking for consent of the Admin-C and Tech-C is explained by the Defendant’s attorney of record in its “GDPR Domain Industry Playbook” provided to German eco Domain Society as follows:

“There are risks associated with proof, such as potentially coupling consent with a domain name registration and withdrawal.” (GDPR Domain Industry Playbook, p. 11)

and

“Since processing based on consent bears a high risk for the parties involved, and may not even be possible for certain types of processing, the model described in this paper will not include any suggestions for consent-based processing. While it is possible that parties involved will introduce such processing, consent-based processing should not be mandatorily required by ICANN due to its associated risks.” (GDPR Domain Industry Playbook, p. 13)

We submit said GDPR Domain Industry Playbook as

- **Appendix AS 9** -.

It cannot go without saying, at no point in said Playbook, nor in its protective letter, does the Defendant (or his counsel) explain the alleged “risks” associated with collecting the Admin-C and Tech-C data based on consent. What is apparent is that the collection of the consent creates some work load on the Defendant as the domain registration process has to be changed. Thus, the Defendant wishes to no longer collect any Admin-C and Tech-C data because the Defendant suggests that the collection of consent would be complex. However, such alleged “complexity” is provided for by the law maker, therefore, Defendant cannot argue that complying with legal obligations associated with obtaining consent render obtaining such consent an undue burden.

II. The legitimate purpose of collecting the data

The Chamber has not duly considered the relevant legitimate purpose of collecting Admin-C and Tech-C data. And when reassessing the Chamber has to consider that the law maker made the requirement of a legitimate purpose within the meaning of Art. 5 (1) b) GDPR a very broad requirement.

1. The purpose of collecting Admin-C and Tech-C data

The Applicant requires through contract that those like the Defendant provide the option to registrants – without a corresponding obligation – to name an Admin-C and Tech-C different to the registrant. This give the registrant the possibility to route certain communication, i.e., administrative or technical communication, to the person deemed fit to handle those issues by the registrant. These contacts may be also a third service provider like an attorney who is liable for taking care of proper communication. The purpose is therefore – as the Chamber also acknowledges in its court decision – comparable to the role of an attorney or trademark assistant for the trademark owner.

In its protective letter the Defendant even confirms that the option to provide separate Admin-C and Tech-C data has legitimate reasons. According to Appendix AG 1 submitted by Defendant, there are approximately 10 million domain name registrations with the Defendant’s group of companies and that for nearly 5 million of such domains the information for the registrant differs with the information provided for the Admin-C and/or Tech-C:

“When comparing the available data of domain holder, Admin-C and Tech-C for approx. 10 million registered domains of our registrar Tucows Domains

Inc., also belonging to the Tucows Group, an ICANN-accredited registrar, it turns out that in significantly more than for half of all registered domains, the e-mail address of the domain owner is identical to the one of the Admin-C and Tech-C. In more than three quarters of all cases even all given information for name, surname, organization, address and e-mail between holder and Admin-C are completely identical.” [Emphasis added]

This affidavit is an impressive demonstration of the relevance for registrants to have the **option** to name a different Admin C and/or Tech C. The statement that in “*more than for half of all registered domains, the e-mail address of the domain owner is identical to the one of the Admin-C and Tech-C*” means at the same time that in almost half (approximately 5 million) of the domain registrations of Tucows Domains Inc. the registrant elected to name an Admin-C and Tech-C different than the registrant.

From the statement “*In more than three quarters of all cases even all given information for name, surname, organization, address and e-mail between holder and Admin-C are completely identical.*” it follows that in around one quarter (approximately 2.5 million) of all domain registrations registered by Tucows Domains Inc. the registrant elected to name a different Admin-C. While the affidavit does not provide a number regarding the Tech-C it is apparent from these two statements together that the number of registrations where the Tech-C differs from the registrant is even higher than for the Admin-C.

These figures evidence that a large number of registrants make use of the option to name a different Admin-C and/or Tech-C. We also depict below a summary on the roles of the administrative and technical contacts provided by different registrars evidencing the acceptance of such roles in the market. Some registrars even go as far as recommending not to name the same person as Admin-C and Tech-C in order for the Tech-C to

“act as a secondary or backup administrator for a domain in the absence of the owner/administrator with respect to the single most often needed modification of a domain: the assignment of the name server.”

We have depicted this passage found on <https://www.bestregistrar.com/faq/a6.jsp>, as well as other descriptions hereafter:

Administrative Contact

The domain name administrator is the person or role who will have full authority to request and authorize any necessary decisions and updates on behalf of the domain owner, including contact information and name server information, for the chosen domain name. The administrator should be familiar with the plans for the domain name and how it will be used. The administrator is usually, though not always, the owner of the domain name. If it is not the owner, he or she is the representative of the owner. The registrant of a domain should take special care in selecting an administrative contact, since a domain administrator has authority almost equal to that of the owner on decisions concerning the domain, including transferring ownership. If there is a dispute, only the owner of the domain can override the administrator's decisions.

Technical Contact

Usually, the technical contact is the person, role, or organization responsible for the web server on which a domain is hosted. The technical contact has the authority to update name server information, and attend to the technical administration of the domain files on the server. He/she does not have the authority to transfer ownership or administrative rights.

It is usually not advisable to for the technical contact to be the same person as the administrator, although that is certainly allowed and often done. A technical contact can act as a secondary or backup administrator for a domain in the absence of the owner/administrator with respect to the single most often needed modification of a domain: the assignment of the name server.

Good choices for technical contact could include the webmaster or web designer for the domain, or someone at your Internet Service Provider or web hosting service.

<https://www.bestregistrar.com/faq/a6.jsp>)

and

The **Administrative Contact** is the licensee's appointed agent for the functions above and any other purpose. In the case that the Registrant is a company the Administrative Contact should be an employee, director, manager of the company. This person has full authority for all changes in our system so care should be taken in selecting the appropriate person to nominate for this role.

The **Technical Contact** is the person responsible for maintaining the DNS nameservers associated with the domain name. This enables that contact to make updates if necessary if, for example, the name of the DNS nameserver changes.

<https://vcgcorporate.zendesk.com/hc/en-us/articles/214821983-What-is-a-registrant-administrative-technical-billing-contact->)

and

The Admin Contact will receive notifications regarding the domain name expiration and will need to approve any transfers for the domain name. This is also the contact listed with the Whois database unless Direct Privacy is enacted.

The Technical Contact is responsible for maintaining and updating the DNS name servers associated with the domain name.

<https://directnic.com/knowledge/article/73:what+is+the+role+of+each+domain+name+contact%3F>)

We attach respective excerpts as

- Appendix AS 10 -.

Lastly, the Admin-C's role is also confirmed by Tucows Domains Inc.'s, which is a part of the same group of companies as the Defendant, Master Domain Registration Agreement:

“TRANSFER OF OWNERSHIP. The person named as Registrant on record with Tucows shall be the "Registered Name Holder." If designated, the person named as administrative contact at the time the controlling account

was secured shall be deemed the designate of the Registrant with the authority to manage the domain name. [...]

We submit a copy of the Master Domain Registration Agreement as

- Appendix AS 11 -.

Such option serves also the purpose to make sure that the domain name registration is managed by experts being in the position to react immediately in case of security issues, legal issues or mere technical problems in connection with such domain name registration.

The Defendant deprives the registrant of such possibility to name a third person – whether a legal entity or a natural person – **as Admin-C and Tech-C**. Even in case of explicit consent of the data subject of the Admin-C and Tech-C data elements, the registrant cannot provide details for the Admin-C and Tech-C as the Defendant will simply not collect such data elements.

2. Broad interpretation of legitimate purpose

The Art. 29 Working Party has issued a variety of working papers and guidelines regarding the GDPR.

The Art. 29 Working Party was an advisory body made up of representatives from each data protection authority of each European Union member state, the European Data Protection Supervisor and the European commission (with the GDPR taking effect the Art. 29 Working Party was replaced by the European Data Protection Board). On 2 April 2013 the Art. 29 Working Party issued an in depth opinion on the principle of “purpose limitation” (hereinafter “**WP 203**”). While such opinion was issued in relation to the Directive 95/46/EC, i.e., the directive repealed by the GDPR, the principle remained. The WP 203 is endorsed in the guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, i.e. GDPR. (the “**WP 253**”, p. 11). WP 253 - and thereby also WP 203 - is also expressly endorsed by the European Data Protection Board, which as noted above replaced the Art. 29 Working Party on May 25, 2018. We submit WP 253 and WP 203 and the European Data Protection Board’s endorsement as

- Appendix AS 12 -.

In WP 203 “legitimate purpose” is described as a broad requirement:

“The requirement of legitimacy means that the purposes must be 'in accordance with the law' in the broadest sense. This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts.

Within the confines of law, other elements such as customs, codes of conduct, codes of ethics, contractual arrangements, and the general context and facts of the case, may also be considered when determining whether a particular purpose is legitimate. This will include the nature of the underlying relationship between the controller and the data subjects, whether it be commercial or otherwise.”

III. The specified and explicit purpose of collecting the data

When reassessing the requirements of Art. 5 GDPR the Chamber has to consider that the purpose at hand is clearly specified and explicitly mentioned.

Sec. 4.4.7 of the Temporary Specification issued by the Applicant states that collection of such data is required to enable the publication of technical and administrative points of contact administering the domain names at the request of the Registered Name Holder. According to the Temporary Specification, the data indicated for these points of contacts is shown as REDACTED for privacy if personal data is concerned and will only be made available: a) if the contact has given his consent; or b) to interested third parties having a legitimate interest upon request (see below VII). Having the Admin-C or Tech-C points of contact available when the registrant is not able or willing to take care of managing his domain name registration(s) ensures that a mechanism for communication is established (see Sec. 4.4.5 and Sec. 4.4.6 Temporary Specification).

The collection of technical and administrative points at the same time are essential part of the domain name system, which the Applicant coordinates. The collection of these contacts serve the objectives of a secure domain name system including, but not limited to, the legitimate purposes of consumer protection, investigation of cybercrime, DNS abuse and intellectual property protection (Sec. 4.4.8 Temporary Specification) and it provides a framework to address appropriate law enforcement needs (Sec. 4.4.9 Temporary Specification). Admin-C and Tech-C data collection serves these objectives. It is recognized practice in order to achieve these objectives that registrants have the option to delegate its tasks and rights to experts by naming them as Admin-C and Tech-C. And, if they do so, it is crucial that registrars, such as Defendant, collect their data so that law enforcement authorities, for example cybercrime units in case of a virus attack or public prosecutors in case of child abuse content, or trademark

owners in case of deception of consumers about the origin of products, actually know what person is taking care of administrative and technical issues regarding the domain name.

IV. Data necessary to collect in relation to the purpose

The data to be collected *may be* personal data if the registrant wishes to provide personal data of a natural third person to be contacted in case of administrative or technical issues. Thus, it is up to the registrant – in coordination with the third person - to refer to additional personal data of a natural third person.

In order to achieve the purpose, i.e., enabling communication with the Admin-C or Tech-C that the registrant entrusted with administering the domain name and ensuring the other aims indicated above, the collection of the collected data elements is necessary.

This is also not contradicted by the affidavit submitted as Appendix AG 1. Firstly, the affidavit is in direct contravention of the Master Domain Registration Agreement submitted as Appendix AS 11. In the affidavit Mr. Schwertner compares “[...] *the available data of domain holder, Admin-C and Tech-C for approx. 10 million registered domains of our registrar Tucows Domains Inc., also belonging to the Tucows Group, an ICANN-accredited registrar, [...]*”.

In German: vergleicht “[...] *Bestandsdaten von Domaininhaber, Admin-C und Tech-C für ca. 10 Mio. registrierte Domains unseres Registrars Tucows Domains Inc., einem ebenfalls zur Tucows Gruppe gehörenden, ICANN-akkreditierten Registrar, [...]*”

Mr. Schwertner hereto explains “we”, i.e. Tucows Domains Inc. or the Tucows group, of which Defendant is a part,

“only accept instructions in connection with the domain registration agreement from the domain holder, either directly or via the owner of the customer account as an intermediary, whereas we do not accept instructions from the Admin-C or Tech-C.”

This is in direct violation of its own Master Domain Registration Agreement, which stipulates:

“administrative contact [...] shall be deemed the designate of the Registrant with the authority to manage the domain.”

Where its own contracts provide that the administrative contact shall be deemed the designate of the registrant, one cannot at the same time ignore instructions received from such designate.

Even if Defendant may refuse to acknowledge the widely accepted roles of the Admin-C and Tech-C (see above, Appendix AS 10), and not contact the Admin-C and/or Tech-C, this does not mean that also others will not contact the Admin-C or Tech-C regarding technical and administrative issues. For example, pursuant to Sec. 2 of the Rules for Uniform Domain-Name Dispute Resolution Policy (UDRP Rules) the Admin-C and Tech-C shall also receive notice of any complaint under the UDRP to safeguard that the registrant receives actual notice of such a complaint:

“a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

- *(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, **the technical contact, and the administrative contact** and (B) supplied by Registrar to the Provider for the registration's billing contact; and*
 - *(ii) sending the complaint, including any annexes, in electronic form by e-mail to:*
 - *(A) the e-mail addresses for those **technical, administrative, and billing** contacts;*
 - *(B) postmaster@<the contested domain name>; and*
 - *(C) if the domain name (or "www." followed by the domain name) resolves to an active web page (other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and*
 - *(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Applicant under Paragraph 3(b)(v).”*

V. The registrant must obtain consent of the data subject

The Defendant is also contractually obligated to ensure that the registrant has collected required consent. The RAA provides that personal data of third persons such as in connection with Admin-C and Tech-C may only be processed if said third person has consented to the use of its personal data. Pursuant to Sec. 3.7.7.6 RAA, any registrant must represent that it obtained consent of the data subject in case personal data shall be used for the Admin-C or Tech-C:

“3.7.7.6 The Registered Name Holder shall represent that notice has been provided equivalent to that described in Subsection 3.7.7.4 to any third-party individuals

whose Personal Data are supplied to Registrar by the Registered Name Holder, and that the Registered Name Holder has obtained consent equivalent to that referred to in Subsection 3.7.7.5 of any such third-party individuals.”

The requirements for the consent to be obtained are described in Subsection 3.7.7.5 RAA which makes reference to 3.7.7.4 RAA:

“3.7.7.5 The Registered Name Holder shall consent to the data processing referred to in Subsection 3.7.7.4.”

“3.7.7.4 Registrar shall provide notice to each new or renewed Registered Name Holder stating:

3.7.7.4.1 The purposes for which any Personal Data collected from the applicant are intended;

3.7.7.4.2 The intended recipients or categories of recipients of the data (including the Registry Operator and others who will receive the data from Registry Operator);

3.7.7.4.3 Which data are obligatory and which data, if any, are voluntary; and

3.7.7.4.4 How the Registered Name Holder or data subject can access and, if necessary, rectify the data held about them.”

This is consistent with the Temporary Specification, which did not change the stipulations on obtaining consent from the data subjects.

In this context it is important to stress that the critical statement of the International Working Group on Data Protection in Telecommunications cited by the Defendant in its protective letter (p. 9) basically refers to the fact that personal data has been collected without consent of the data subject.

The Defendant, however, is not hindered to require any evidence it may deem fit showing that the Admin-C or Tech-C have consented to the use of their personal data.

VI. Collection of data for contractual fulfillment

As a consequence of the contractual obligation mentioned above, the Defendant has to provide the option to the registrant to name a different person as an Admin-C and Tech-C. Where the registrant provides its own data, it shows that it does not wish to exercise that option. Where data of a third person is provided, it shows that and how the option was exercised.

Further, the collection of the data is also necessary for the performance of the legal relationship between the registrant and the third person acting as Admin-C and/or Tech-C. The third person acting as Admin-C and/or Tech-C is granted far-reaching powers by the registrant. The Admin-C and/or Tech-C might take over this role in fulfillment of an employment contract with the registrant or in fulfillment of legal relationship regarding the provision of certain IT-services. Management of a company regularly appoints an IT specialist of the company to act as the Admin-C and/or Tech-C. Even where no employment relationship is present between the registrant and the Admin-C and/or Tech-C, for example in case of appointment of an external service provider acting as Admin-C and Tech-C, their relationship constitutes a mandate (*Auftrag*) within the meaning of Article 662 German Civil Code or where the third person receives payment it constitutes nongratuious management of the affairs of another (*Entgeltliche Geschäftsbesorgung*) within the meaning of Article 675 German Civil Code (see Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2nd edition, § 7 margin 24).

VII. The collection of data is based on legitimate interests

The Chamber has not applied the relevant criteria when assessing the question of legitimate interest of processing personal data.

Providing the option, as required under the RAA (and unchanged by the Temporary Specification), to delegate certain roles to third persons is an offer to the registrant to use third persons to assist in administering the domain name. Involving third persons to perform certain obligations is a legitimate standard, an accepted practice and is a foundation of today's divided labor economy. Consequently, German law provides for categories of third persons such as for example representatives (*Vertreter*), auxillary persons (*Erfüllungsgehilfen*), or assistants (*Verrichtungsgehilfen*).

Whereas it is legitimate in general to entrust third persons to perform certain obligations, it is also legitimate for a registrant to entrust third persons to act as Admin-C and Tech-C. Most important, the Chamber has not considered that the registrant makes use of an option on its free will. Further, the Admin-C and Tech-C, if different from the registrant, choose to assume such roles at their own free will. As explained above, the Admin-C has full authority to request and authorize any necessary decisions and updates on behalf of the registrant, including contact information and name server information, for the chosen domain name. The Tech-C has the authority to update name server information. Where the Admin-C and Tech-C have such far reaching powers, collection of the data elements specified in the motion is required to identify and contact the Admin-C and Tech-C. And the person who assumed the Tech-C or Admin-C role also expects its data to be collected. If it were not collected, it could not serve in this role as there was no way for such person to legitimize itself and show that it was entrusted to act as Admin-C and/or Tech-C.

Furthermore, such collection of data is also crucial for the objectives of a secure domain name system, including but not limited to the legitimate purposes of consumer protection, investigation of cybercrime, DNS abuse and intellectual property protection and law enforcement needs. The Chamber cannot ignore that the current system provides the option to name Admin-C and Tech-C data. As a consequence, millions of domain name registrations are managed by respective administrative and technical contacts not being the domain name registrant. In all of these cases it is important for cybercrime units to identify the persons actually controlling the domain name registration and respective content. It is also important to have the option to immediately contact the person taking care of technical issues of the domain name registration. According to German law these persons are also liable for the content or have to provide certain information on the domain name registration and its content towards law enforcement authorities or trademark owners. We refer to our references made in our application on page 13. Therefore, the Chamber cannot ignore that collection of Admin-C and Tech-C data is based on legitimate interests.

VIII. Additional consent is necessary for publication of Admin-C and Tech-C data

The Chamber has stated in its facts that

“Under so-called WHOIS service the data collected during new domain name registrations are published on a publicly accessible internet portal for identification purposes.”

In German:

“Unter dem sog. WHOIS” Service werden die im Zusammenhang mit Neuregistrierungen erhobenen und gespeicherten Daten zu Identifizierungszwecken auf einem öffentlich zugänglichen Internetportal veröffentlicht.”

The Defendant has referred to statements in its protective letter in which Art. 29 Working Group has criticized full publication of WHOIS data in the past (see page 8).

While the further processing of the data in dispute is not subject to this dispute, the Applicant would like to clarify and evidence that the Applicant has implemented the necessary safeguards to ensure WHOIS publication in compliance with the GDPR:

The data elements relating to the Admin-C and Tech-C will **not be publicly accessible without consent** pursuant to Sec. 2.4 Temporary Specification:

“2.4. In responses to domain name queries, Registrar and Registry Operator MUST treat the following fields as "redacted" unless the contact (e.g., Admin, Tech) has provided Consent to publish the contact's data:

*Registry Admin/Tech/Other ID
Admin/Tech/Other Name
Admin/Tech/Other Organization
Admin/Tech/Other Street
Admin/Tech/Other City
Admin/Tech/Other State/Province
Admin/Tech/Other Postal Code
Admin/Tech/Other Country
Admin/Tech/Other Phone
Admin/Tech/Other Phone Ext
Admin/Tech/Other Fax
Admin/Tech/Other Fax Ext”*

To nevertheless enable third parties to contact the Admin-C and Tech-C, the Temporary Specification provides in Sec. 2.5 that an anonymized way of communication must be made available:

“2.5. In responses to domain name queries, in the value of the "Email" field of every contact (e.g., Registrant, Admin, Tech):

*2.5.1. Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, **MUST NOT identify the contact email address or the contact itself.***

*2.5.1.1. The email address and the URL to the web form **MUST provide functionality to forward communications received to the email address of the applicable contact.***

Pursuant to Sec. 4 of the Temporary Specification, access to the data elements collected in relation to the Admin-C and Tech-C only need to be made available where the requirements of Article 6(1)f GDPR are satisfied or where there is guidance that making such data available is lawful:

4. Access to Non-Public Registration Data

*4.1. Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to third parties on the basis of a legitimate interests pursued by the third party, except 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.***

4.2. Notwithstanding Section 4.1 of this Appendix, Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to a third party where the Article 29 Working Party/European Data Protection Board, court order of a relevant court of competent jurisdiction concerning the GDPR, applicable legislation or regulation has provided guidance that the provision of specified non-public elements of Registration Data to a specified class of third party for a specified purpose is lawful. Registrar and Registry Operator MUST provide such reasonable access within 90 days of the date ICANN publishes any such guidance, unless legal requirements otherwise demand an earlier implementation.
[Emphasis added]

These efforts to ensure the compliance of the WHOIS system were also explicitly recognized by the Article 29 Working Group during its plenary meeting of 25 May 2018.

B. LEGAL ASSESSMENT

Contrary to the opinion of the Chamber, the Applicant has substantiated the claim for the requested interim injunction under application 1 (*Verfügungsanspruch*) (see I). Even if the Chamber upheld the position expressed in the Decision, it would have to issue an injunction, if necessary with a clarifying restriction in accordance with the alternative application (see II). There is also a reason for the injunction (*Verfügungsgrund*) (see III). If the Chamber does not remedy the immediate appeal and the Senate has doubts about the existence of the claim for an injunction, Applicant requests that the Senate submit the questions it considers to be legally relevant to the ECJ for preliminary decision (see IV), in a case which is of considerable importance for the Applicant, as well as for all parties to the domain system developed by it (see V).

I. The legal basis for the injunction under application no. 1)

Contrary to the legal opinion of the Chamber, the claim for injunction exists according to the application under no. 1.).

It is undisputed that the Defendant has a contractual obligation arising under the RAA to collect Admin-C and Tech-C data when a domain is registered.

However, the Regional Court rejected the claim for injunctive relief under the contract with the reasoning that the collection of the data was not necessary, referring to Art. 5 (1) b) and c) GDPR. However, the Regional Court ignores the fact that there are various legal ways to collect this data and the collection is indeed necessary to achieve the purpose set by the Applicant. If there is even only one legal way to collect the data in dispute (and there are several ways to do so in this case), the claim to injunction cannot be denied. If there is even just one way, the

obligor, in this case the Defendant, must choose this one way. Only because a contractual obligation may also be fulfilled in an unlawful manner, it does not follow, as the Regional Court seems to have assumed, that the obligor, in this case the Defendant, can also refuse performance in a lawful manner.

First, the Defendant can undoubtedly and in any event fulfill its obligation to collect the Admin-C and Tech-C data in dispute as the agreement does not even require the collection of personal data as Admin-C and Tech-C data (see 1.). Second, the Defendant can fulfil its obligation to collect the data in dispute even if the data constitute personal data of a natural person (see 2.).

1. The collection of Admin-C and Tech-C data is lawful – no obligation to collect personal data

There is no question that collection of Admin-C and Tech-C data is lawful. As an initial matter, the information about the Admin-C and Tech-C need not be information about natural persons; such data can also be about legal persons or a role (i.e., domain administrator). Nothing in the RAA or the Temporary Specification requires collection of personal data about a natural person for the Admin-C and Tech-C.

The GDPR only applies if data of natural persons are concerned (cf. already the title of the GDPR, which speaks of the protection of natural persons; application p. 18; cf. also recital 170 of the GDPR). Recital 14 of the GDPR also reads:

This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

Accordingly, the GDPR is irrelevant if no data about natural persons are collected. In this respect, the Defendant is contractually obliged to collect such data, and failure to do so violates its contract with the Applicant. Indeed, the application for a preliminary injunction is not directed at the collection of personal data, but rather the collection of Admin-C and Tech-C data. However, the Defendant has declared that it will not collect any Admin-C or Tech-C data, regardless of whether or not it is personal data.

The Chamber nevertheless rejects the claim for injunction as a whole. It thus argues that the collection of Admin-C and Tech-C data is in conflict with the GDPR, even where the GDPR does not apply to this factual background. Out of legal precaution, the Applicant

has therefore made this situation the subject of a separate alternative application for injunction (cf. under II).

2. The collection of Admin-C and Tech-C data is lawful even if personal data is provided

Further, even if the Admin-C and Tech-C data collected is personal data of a natural person, collection of this data is also lawful. All of the requirements under the GDPR that provide for legal collection of personal data about natural persons are easily satisfied in the present circumstances.

According to the GDPR, the following requirements must be met:

The data must be collected for specified, explicit and legitimate purposes in accordance with Art. 5 (1) b) GDPR (see a)) and the data shall be adequate, relevant and limited to what is necessary in accordance with Art. 5 (1) c) GDPR (see b)). In addition, the data must be processed lawfully pursuant to Article 5 (1) a) in connection with Art. 6 GDPR (see c)).

As noted above, and explained in detail below, all of these requirements can be easily fulfilled:

a. The processing is appropriate (Art. 5 (1) b) GDPR)

The Chamber is of the opinion that the collection of Admin-C and Tech-C data is not necessary to achieve a legitimate purpose (Decision, p. 6 with reference, without further distinction, to Art. 5 (1) b) and c) GDPR).

This view is not tenable. The Chamber has neither correctly understood the legitimate purpose of data collection for the Admin-C and Tech-C, nor has it examined the principle of data minimization in relation to this actual purpose.

The purposes for which certain data are collected are determined by the data controller (Art. 5 (2) GDPR). In particular for the Admin-C and Tech-C data at issue here, the Applicant has stated the following purpose in its Temporary Specification in Sec. 4.4.7:

Enabling the publication of technical and administrative contact points for the management of domain names at the request of the holder of the registered name.

This purpose necessarily includes the collection of the data relating to Admin-C and Tech-C, if so offered by the person registering the domain (see above, Sec. A.II.1.) and leads to the fulfillment of important objectives as *inter alia* establishing communication (see Sec. 4.4.5 and 4.4.6 Temporary Specification). At the same time though, the publication of data is limited in case personal data of natural person is concerned in order to be compliant with GDPR and will only: a) be made public if the data subject consented specifically to this publication; or b) be provided to a third person who proves legitimate interest (see above, Sec. A.VIII).

Furthermore, collection of Admin-C and Tech-C data automatically serves the legitimate purpose of consumer protection, investigation of cybercrime, DNS abuse and intellectual property protection (Sec. 4.4.8 Temporary Specification) and it provides a framework to address appropriate law enforcement needs (Sec. 4.4.9 Temporary Specification).

The Applicant has already explained in detail why Admin-C and Tech-C data collections help to achieve these objectives. The Registrant has the option to delegate its tasks to an expert. And in case of legitimate interest it is crucial for law enforcement authorities or trademark owners to be in the position to find out: a) whether such tasks have been delegated; and b) if so, the identity of that person.

The Applicant has already explained in detail in its request for injunction under IV. 1. and 2. (pages 7/8) that the Applicant pursues these purposes and the advantages they bring.

This purposes are specified, explicit and legitimate within the meaning of Art. 5 (1) b) GDPR:

i. The purpose is specified and explicit

The requirements "specified" and "explicit" complement each other in so far as the first formal requirement relates to what is to be specified explicitly as an "act of self-commitment" (Paal/Pauly, GDPR, 2. Edition 2018, Art. 5 marginal 26; Härting GDPR marginal 95; Wolff in Schantz/Wolff DatenschutzR marginal 402).

The purpose of enabling the publication of technical and administrative contact points, which necessarily includes the collection of the data in the first place, is laid down in the Temporary Specification in Sec. 4.4.7 and is thus specified and explicit.

In addition, Sec. 4.5.1. of the Temporary Specification specifies that the processing of the data identified in the Temporary Specification is necessary to achieve the legitimate

interests identified in the Temporary Specification including such legitimate interests specified in Sec. 4.4.8 and 4.4.9.

ii. The purpose is legitimate

The data is also collected for legitimate purposes.

Both in Art. 6 (1) a) DSRL and lit. a Council of Europe Convention 108, "legitimate" has so far been translated as "lawful" (BeckOK GDPR, Art. 5 marginal 17). However, the new translation of the GDPR ("legitimate") speaks for a broader interpretation.

(1) The Art. 29 Working Party assumes that an objective is legitimate if it is consistent with the legal order as a whole (Art. 29 Working Party, WP 203 v. 2.4.2013, 19 f.). It is therefore not important whether the processing for this purpose is legal pursuant to Art. 6 (1) GDPR, but whether it is an object disapproved of by the legal system (e.g. discrimination against certain groups of persons on racist grounds, cf. Helbig K&R 2015, 145 (146); so also Ehmann/Selmayr, Art. 5 marginal 15). So this is at best a rather broad filter.

It cannot be doubted that the processing of Admin-C and Tech-C data is legitimate according to this interpretation. The division of labor is legitimate and approved by the legal system. Without it, economic life as we know it today would not exist. This option of delegation is also necessary in cases where the domain holder is not able to fulfil the administrative and technical tasks in connection with a domain name. Furthermore, in such case of delegation of work the collection of such data is required to fulfil further legitimate purposes of the domain name system. Third parties need to be able to identify such persons acting as representatives for administrative or technical matters, and third parties, for example law enforcement or trademark owners, need to be able to contact these persons in case of legal or technical issues.

(2) According to another view, a change in the meaning of "legitimate" should be rejected (Paal/Pauly, Art. 5 marginal 28). Accordingly, the wording no longer corresponds to the wording in Art. 6 (1) b) DSRL ("lawful"). However, the wording in the English ("legitimate") and French ("légitimes") versions had remained unchanged (see again Paal/Pauly, Art. 5 marginal 28). In addition, lawful and legitimate should be considered to be equivalent. According to this minority opinion, the purpose is therefore legitimate if the data collection is lawful.

Since this is the case in the present case (cf. under c.), it does not matter which opinion the regional court or the Senate endorses in this regard.

However, if the Senate has doubts about the legitimacy of the purpose of the data collection and considers the question of the interpretation of the legitimate purpose to be controversial and decisive, we request that this question be referred to the ECJ for a preliminary ruling (see IV below).

b. The processing is adequate and limited to what is necessary (Art. 5 (1) c) GDPR)

Contrary to the opinion of the Regional Court (Decision, p. 6), the processing of Admin-C and Tech-C data is adequate for the purposes, also against the background of data minimization.

The Regional Court fails to recognize the specified and explicit purposes in its decision and does not strike the right balance between the question of the need to collect the data and legitimate purposes. The Chamber states that data collection is not necessary to avoid criminal violations of the law or security problems (decision, pp. 6-7). This view is not tenable.

In the first place, the Regional Court's conclusion is incorrect. The collection of Admin-C and Tech-C data – if provided by the registrant - is necessary to improve security of the domain name system giving law enforcement and other third parties the opportunity to identify and contact the Admin-C and Tech-C authorized by the registrant.

Furthermore, the question discussed above becomes relevant in connection with the question of legitimate interest according to Art. 6 (1) f) GDPR (and we will revert to this in Sec. I.2.c.ii below). Instead, Art. 5 (1) c) GDPR asks about whether the data is adequate in order to fulfil the legitimate purpose. The correct question in the context of Art. 5 (1) c) GDPR is therefore whether the data collection is necessary to enable the registrant to name additional technical and administrative contact points for the administration of the domain name.

And this question can only be answered with "yes":

As explained, one purpose of collecting Admin-C and Tech-C data is to give the registrant - if desired - the opportunity to have the registered domain technically and administratively managed, e.g., by a suitable service provider or a specific person working for a legal entity. This is only possible if these persons are actually identified as contact persons for and can be contacted if there is a legitimate interest.

The fact that there is also an actual need for the choice by the registrant to name others than herself as the Admin-C or Tech-C is documented by the affidavit submitted by the Defendant. In particular, there are nearly 5 million of approximately 10 million registered domain names for which the Admin-C and Tech-C are different from the registrant. This is also happening for good reason. The Admin-C and the Tech-C have a legal relationship with the registrant and are therefore the contact point for very different tasks and persons. In the UDRP procedure, for example, proof of effective delivery of a complaint is also provided by sending the complaint to the Admin-C and Tech-C. The Admin-C has monitoring duties according to the jurisdiction of the Federal Court of Justice and can therefore be held liable by a trademark owner as a violator, for example. The Defendant also recognizes the legal relevance of these positions. In its contract with the registrant, it expressly refers to the rights of the Admin-C, who may, among other things, transfer the domain, in accordance with the Sec. Transfer of Ownership of the Master Domain Registration Agreement. If the Admin-C contacts the Defendant instead of the domain holder for the purpose of transferring a domain, the Defendant **has** to deal with the Admin-C (see Appendix AS 11, Section “TRANSFER OF OWNERSHIP”).

The opinion of the Article 29 Group quoted by the Defendant in its protective letter deals with a completely different aspect of the GDPR. It relates solely to the question of which data are to be published as part of WHOIS and when. The mere collection of the Admin-C or Tech-C is not questioned therein. Rather, the Art. 29 Working Group recently endorsed the implementation of the Applicant’s Temporary Specification and respective structure of the domain name system, including WHOIS, ensuring compliance with data protection law provisions.

This possibility should remain open to registrants as the collection of data, if provided, is also appropriate to achieve the purpose. The principle of data minimization consists of three requirements for data processing, which are all geared to the purpose of data processing and together reflect the three stages of the proportionality test (Beck OK GDPR, Art. 5 marginal 24). These are fulfilled without any problems:

i. The data is relevant

First of all, the data must be relevant for the purpose pursued. In the context of the proportionality test, this corresponds to the question of whether the processing of personal data of a natural person is suitable to achieve a legitimate objective (Beck OK GDPR, Art. 5 marginal 24).

The processing of the Admin-C and Tech-C data provided by the registrant is suitable to contact the person indicated and thus to achieve the goal set out above. It is ensured that

the domain name registration is associated with additional technical and administrative contacts in addition to the registrant, if appropriate in the discretion of the registrant.

ii. The data is limited to what is necessary

In addition, the processing of personal data must be limited to what is necessary for the purposes pursued (cf. Ehmann/Selmayr, Art. 5 marginal 22). In this respect, the principle of data minimization traces the elements of necessity, which is included in all legal bases of Art. 6 (1) GDPR (with the exception of consent). Finally, the personal data processed must be adequate. This goes beyond mere relevance for the purpose and requires an evaluation of whether the processing of data to this extent is, in a narrow sense, proportionate (BeckOK GDPR, Art. 5 marginal 26; Paal/Pauly/Frenzel, Art. 5 marginal 35; Dammann/Simitis DSRL Art. 6 marginal 11).

This prerequisite can also be answered in the affirmative.

In this case, only data are collected which lead to the identification of the specified Admin-C or Tech-C. In case of a legitimate interest, entities such as law enforcement authorities or trademark owners need such contact details of the Admin-C and Tech-C in order to identify that person and in order to be able to contact that person as necessary.

However, no data is collected which has no connection with the legitimate purpose. The data collected is therefore limited to what is necessary. The processing of the Admin-C and Tech-C data collected in each case is therefore also necessary and also in the narrower sense proportionate.

The processing of the data thus takes place – contrary to the opinion of the Chamber – in accordance with Art. 5 (1) b) and c) of the GDPR.

c. The processing is lawful (Art. 5 (1) a) in connection with Art. 6 GDPR)

Further, the condition of a justification according to Art. 6 GDPR for the processing of personal data is also satisfied.

The Chamber did not consider the arguments put forward by the Applicant as to the lawfulness of data processing. The Applicant therefore refers to its request for a preliminary injunction (B. I. 2-4, p. 18-22) and adds the following:

Recital 40 of the GDPR states that processing is lawful if the personal data are processed with the data subject's consent or some other legitimate basis laid down by law, either in

this Regulation or in other Union or Member State law as referred to in this Regulation. Art. 6 (1) GDPR incorporates this principle by requiring that one of the legal bases regulated therein must be satisfied.

In the present case, personal data of natural persons relating to the Admin-C and Tech-C data pursuant to Art. 6 (1) GDPR are only collected if this processing is consented to (i. below). In addition, the collection is required for the fulfilment of the legal relationship between the registrant and the Admin-C or the Tech-C (below ii.). Finally, there is also a legitimate interest in the corresponding data collection (iii. below).

i. The data is processed with consent of the data subjects - Art. 6 (1) a) GDPR

The collection of personal data of natural persons relating to Admin-C and Tech-C is voluntary. The data is only processed if the registrant specifies these details during registration, whereby the registrant must obtain the consent of the person concerned, 3.7.7.6 RAA.

If the registrant provides personal data of a third party, the registrant must confirm that it has obtained proper consent. If the Defendant has any doubts about this, it is not prevented from obtaining proof of consent.

It should also be mentioned that personal data will only be published via the WHOIS system if the Admin-C or the Tech-C has also agreed to this publication. Otherwise, the data in WHOIS will be replaced by "REDACTED FOR PRIVACY", Sec. 2.2 of the Temporary Specification. Contact can still be established via an anonymous e-mail or web form, Sec. 2.5.1 Temporary Specification.

Finally, the registrar (the Defendant) may give the Admin-C and the Tech-C the opportunity to consent to the publication of additional contact information in accordance with Sec. 2.4 of Annex A (Sec. 7.2.2 Temporary Specification).

As a result, the collection of personal data is ultimately dependent on consent. Such personal data will only be published if explicit consent has also been given for this publication. The processing of the data is thus covered by consent and thus lawful within the meaning of Art. 6 (1) a) GDPR.

This consent does not contradict the prohibition of coupling in Art. 7 (4) GDPR because the registration remains possible without the indication of personal Admin-C and Tech-C data of a natural person. The registrant can also take on the role of Admin-C and Tech-C himself or name a legal entity. It is only an additional service of the registrar that if

necessary a third party can take over the role of Admin-C and Tech-C and then appropriate information is given.

Consequently, the Defendant can fulfil its contractual obligation to collect Admin-C and Tech-C data in any case by obtaining the consent of the affected data subjects if they are natural persons, or by the registrant providing non-personal data as the administrative or technical contact.

The Defendant does not mention this option in her protective letter. However, a statement by the Defendant's attorney of record in another context shows that at least the attorney of record does not like this solution because its practical execution is to be implemented in an electronic process and this would involve effort. In Defendant's attorney of record opinion, as found in his GDPR Domain Industry Playbook is worded as follows:

"Since processing based on consent bears a high risk for the parties involved, and may not even be possible for certain types of processing, the model de-scribed in this paper will not include any suggestions for consent-based processing. While it is possible that parties involved will introduce such processing, consent-based processing should not be mandatorily required by ICANN due to its associated risks." (GDPR Domain Industry Playbook, p. 13)

However, this opinion does not say that obtaining consent is not possible. On the contrary, it implies that it is possible to obtain this information by changing the registration process accordingly.

ii. Required for performance of a contract - Art. 6 (1) b) GDPR

Furthermore, the processing of Admin-C and Tech-C data is also legal because it is necessary for the performance of a contract to which the data subject is a party.

The wording "fulfilment of a contract" makes it clear that the applicability of Art. 6 (1) b) GDPR does not depend on the contractual partner of the data subject and the person responsible for processing the data being identical (cf. also recital 44). Rather, the wording states that the party concerned is a contracting party. Accordingly, Art. 6 (1) b) GDPR may also legitimize data processing by uninvolved third parties to the extent that this is necessary for the performance of a contract to which the data subject is a party (BeckOK GDPR, Art. 6 marginal 30). This requirement applies if the contract could not be fulfilled to the full extent without processing the data (Paal/Pauly, Art. 6 marginal 14).

That is the case here.

There are legal relationships between the registrant and the Admin-C or Tech-C regarding the taking over of the corresponding tasks for the registrant. Often there will be a service contract with a service provider or perhaps the specified person has an employment relationship with a legal person. Otherwise at least a mandate (*Auftrag*) within the meaning of Article 662 German Civil Code or where the third person receives payment it constitutes nongratuitous management of the affairs of another (*Entgeltliche Geschäftsbesorgung*) within the meaning of Article 675 German Civil Code (see Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2nd edition, § 7 marginal 24) exists between domain name registrant and Admin-C and Tech-C. In order to fulfil the corresponding obligations the Admin-C or Tech-C data must be processed, otherwise the Admin-C or the Tech-C cannot fulfil the tasks taken on because they cannot be contacted due to a lack of data.

Consequently, the collection of the data serves the fulfillment of a contract and the limited contact data collected is also necessary for this contract fulfillment.

iii. Legitimate interest - Art. 6 (1) f) GDPR

Furthermore, data processing is also permitted in accordance with Art. 6 (1) f) GDPR. The processing of any personal data is also in the legitimate interest of the controllers and third parties, Art. 6 (1) f) GDPR.

According to Art. 6 (1) f) GDPR, the processing of personal data is permissible if:

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.

Art. 6 (1) f) GDPR is the central balancing of interests clause of the GDPR, which contains an independent provision of permission and is not to be regarded as a "last resort" (cf. BeckOK GDPR, Art. 6 marginal 45; Ehmann/Selmayr, Art. 6 marginal 15; Art.29 Data Protection Group, WP 207, p. 11 and p. 62). The provision requires the legitimate interests of the person responsible or of a third party to be weighed against the interests, fundamental rights or freedoms of the person concerned (cf. Recital 47 to the GDPR; Ehmann/Selmayr, Art. 6 marginal 22). According to the wording of Art. 6 (1) f) GDPR ("*unless the interests, fundamental rights and freedoms of the person concerned*

[...]), the burden of proof with regard to the rights of the data subject lies with the person concerned. (BeckOK GDPR, Art. 6 marginal 52).

The legitimate interest of the controllers and third parties in the processing of personal data of a natural person, if provided, outweighs that of the Admin-C or Tech-C.

The “legitimate interest” of the controller or third parties to be weighed up must be broadly defined (BeckOK GDPR, Art. 6 marginal 48). Examples of a legitimate interest are fraud prevention, direct marketing (recital 47 on the GDPR) or ensuring network and information security (recital 49 on the GDPR).

When weighing up the interests of the data subjects, "reasonable expectations [...] relating to their relationship with the person responsible" must also be taken into account. It must also be taken into account whether the "data subject can reasonably foresee at the time when the personal data are collected and in view of the circumstances in which they are collected that processing for this purpose may take place" (recital 47 of the GDPR).

The legitimate interest of the controllers and/or the third parties results from the following considerations:

First, the registrant, the Applicant and any third party have a legitimate interest in data processing, which helps to ensure the secure functioning of the Internet's domain name system. The Applicant has already explained in detail why it is important for the registrant to be able to delegate tasks relating to the domain name to an Admin-C or Tech-C. These functions are an essential part of the domain name system. Also, the data serves to support a framework to address issues relating to consumer protection, investigation of cybercrime, DNS abuse and intellectual property protection and helps to accomplish law enforcement needs (see Sec. 4.4.8 and 4.4.9 Temporary Specification).

Second, a legitimate interest of both the registrant and any third party in data processing arises from the fact that the Admin-C and Tech-C give the registrant the opportunity to effectively address abusive acts. If, for example, a website is compromised or a formerly reputable e-mail server begins to send spam or a company's systems are infected with a virus (together "online fraud"), it is of particular importance for averting further damage that those places that can provide relief are informed without delay. This is often the Admin-C and Tech-C. Especially when the registrant considers it necessary to name an Admin-C or Tech-C, for example because the domain holder is a large company (which is difficult to reach under the specified domain holder contact data) or a natural person (who does not have sufficient technical experience), it is particularly important to collect the data of Admin-C or Tech-C. In these cases, the registrant may not be able to stop the

online fraud in time, so that the damage is perpetuated by the delay, for example when an infected computer system as part of a botnet starts to spread harmful viruses itself. If one followed the opinion of the Regional Court of Bonn, then in all these cases the registrant would have to be contacted first, whose reaction would probably be considerably slower, especially in the cases described. Also, another legitimate interest is the protection of children, which is enhanced because those who are purveying child pornography can be better tracked if there is more information about those involved with the domain name.

Third, a legitimate interest of both the registrar and any third party arises from the fact that, in case the registrant is located abroad, the Admin-C can act as domestic administrator of the domain, who - this is in the interest of the registrar - can, for example, renew the domain name with the registrant or, if the registrant automatically renews the domain, can ensure that renewal fees are paid, so that the domain name is not lost. For third parties, in the case of foreign domain name holders, the Admin-C is a domestic contact person who may be easier to contact than the domain name holder, who can also act as the domain name holder's authorized representative in Germany (BeckOK MarkenR/Thalmaier MarkenG § 15 Rn. 173, beck-online) and who – in addition to the foreign domain name holder who might be difficult to get ahold of – is to a certain extent liable for the domain (Hoeren/Sieber/Holznagel MMR-HdB, Part 18.2, marginal 79c, beck-online).

Fourth, a legitimate interest of third parties arises if and when trademark holders are trying to find those who are infringing their trademark through a domain name or tracing the sale of counterfeit goods. In these cases, the data collected if and when offered gives more information on how to contact the person who has registered and /or using the domain name.

In order to protect the stated legitimate interests, the processing of the Admin-C and Tech-C data is also required within the meaning of Art. 6 (1) f) GDPR. This is the only way for the registrant to use the opportunity to delegate these tasks and to ensure the security of the system. Moreover, this is the only way to effectively address abusive actions.

The legitimate interest of the controllers and third parties understood in this way must be weighed against the interests, fundamental rights or fundamental freedoms (in particular Art. 7 and 8 of the CFR Charter) of the person concerned. The interests of the Admin-C and the Tech-C **do not outweigh the legitimate interest** of the controller and third parties in the present case, for the following reasons:

First, the person designated as Admin-C or Tech-C acquires rights. This cannot be done completely anonymously. The person designated as Admin-C or Tech-C is regularly familiar with the operation of the domain name system; otherwise, such person would not take the respective role. The fact that the registering party passes on its personal data to the registrar, which communicates them to the registry operator, therefore corresponds to the "reasonable expectations" of the Admin-C or Tech-C concerned within the meaning of recital 47 of the GDPR. The Admin-C or Tech-C regularly has a legal relationship with the registrant, so that the latter can "reasonably foresee" in view of the circumstances in recital 47 that his personal data, if provided but which is not required, will be processed as described.

Second, even if this is not the subject matter of this proceeding, personal data will only be published through the WHOIS system if the Admin-C or the Tech-C has consented to its publication (see above, Sec. A.VIII.). Otherwise, according to the Temporary Specification, contact must be guaranteed by an anonymous e-mail address or a web form.

The mere collection of Admin-C or Tech-C data – without its publication – does not infringe the rights (in particular the fundamental rights under Articles 7 and 8 of the GR Charter) of the data subject to the same extent as if this data was published without restrictions. The collection of this data is a mandatory consequence of the fact that the third party assumes the role of Admin-C or Tech-C.

Third, recital 49 of the GDPR expressly provides for the prevention of fraud (see example above on online fraud) as well as network and information security as legitimate interests. These are clearly more important interests than "direct marketing", which is also considered a legitimate interest (recital 47).

Fourth, Sec 4.5. of the Temporary Specification provides for specific measures to ensure the proportionality of data processing with regard to the weighing of interests pursuant to Art. 6 (1) f) GDPR:

4.5.1 Processing of the limited personal data referred to in this Temporary Specification is necessary to achieve the identified legitimate interests, as documented in many comments and opinions of interest groups during a 12-month Community consultation. This processing includes in particular the storage of personal data already collected and the ongoing collection of personal data;

4.5.2 The multi-level access framework for RDDS identified in the interim model and implemented in this Temporary Specification was specially

developed to minimize the intrusiveness of processing while still enabling the necessary processing;

4.5.3 Processing within the tiered/layered access framework according to this Temporary Specification minimizes the risk of unauthorized and unjustified processing;

4.5.4 This Temporary Specification contains requirements to ensure that the holders of registered names are informed of the intended processing and of their rights in relation to such processing;

4.5.5 This Temporary Specification contains requirements to ensure that adequate records are kept of processing activities in order to meet the accountability obligations set out in the GDPR.

Finally, in the context of weighing up interests, it must also be taken into account that the legal basis allowing the processing under Article 6 (1) f) GDPR is flanked by the procedural obligation to inform the person concerned of the (legitimate) interests, cf. Article 13 (1) d) and Article 14 (2) b) GDPR. The persons concerned by the data processing are also entitled to a right of objection in accordance with Art. 21 GDPR (Ehmann/Selmayr, § 6 marginal 5; BeckOK DatenschutzR/Albers DS-GVO Art. 6 marginal 45-54, beck-online). Therefore, even the scenario – which is only theoretical – that the personal data of a Tech-C or Admin-C is held against their will is excluded.

All these circumstances lead to an appropriate balance between the legitimate interests of third parties and the interests, fundamental rights and freedoms of the Tech-C and Admin-C. The court has also acknowledged such legitimate interest comparing the situation with a trademark register and cited representatives of the trademark owner, without assessing justification of the use of data under Art. 6 (1) f) GDPR though.

The data processing is therefore also lawful in accordance with Art. 6 (1) f) GDPR.

From the Applicant's point of view, the other requirements of the GDPR are obviously fulfilled or not decisive for the injunction applied for here and are also not disputed by the Defendant within the scope of the protective letter. If the Chamber or the Senate nevertheless deems further submissions on certain prerequisites of the GDPR necessary, the Applicant kindly asks for a corresponding judicial note.

II. On the alternative claim - discretion of the court according to § 940 ZPO

The Applicant has already explained that it is up to the Defendant to fulfil its contractual obligation in such a way that this is done in a lawful manner. Therefore, there is no reason for the Chamber or the Senate to limit the claim under 1).

1. Discretion of the court, § 940 ZPO

The Applicant acknowledges the power of the court to render a decision at its own discretion in order to ensure the purpose pursued by the Applicant is met. The Applicant would like to stress again its opinion that such protection of interest requires an order according to application for relief under 1.). If the Chamber, however, holds that only the collection of the data elements in a certain way as lawful, this may be expressed by issuing a decision containing corresponding restrictions. The Applicant also submits a restricted wording as an alternative application for relief as follows. It reserves its right though to proceed with this immediate appeal in case that application for relief according to 1.) is dismissed.

2. The alternative application for relief no. 2)

The alternative application for relief according to 2) provides for the collection only if the consent of the Admin-C and Tech-C for the collection of this data has been obtained for the purpose of enabling contact for administrative and technical matters or if no personal data of a natural person is concerned in the first place.

This application is limited to what the Chamber must accept as necessary, irrespective of what interpretation of the GDPR it follows. Because even after the strictest reading of the GDPR imaginable, it can and must be lawful to provide your contact details voluntarily and with your consent, because you want to act for the (legitimate) purpose of providing services for the registrant. For this purpose it is also necessary to collect the contact data stated in the application, as this is the usual way of establishing contact today. Furthermore, this data is necessary for the clear identification of the Admin-C and the Tech-C, if they themselves are liable for infringements. The injured party must therefore be able to identify the Admin-C or Tech-C if there is a legitimate interest in doing so. If there are concerns about the need to collect a specific data element, the Chamber may remove that element from the list shown in the application.

Furthermore, the processing must also be possible if no personal data relating to a natural person is concerned as the GDPR does not even come into play in that scenario.

Essentially, the Defendant wants to abolish the role of Admin-C and Tech-C by no longer collecting any data.

III. Reason for injunctive relief

The Applicant has set out in its application for issuing a preliminary injunction the reasons for injunctive relief (see application, p. 22-23). The facts of the case are undisputed; the Defendant has once again expressly confirmed in the protective letter of 28 May 2018 that it "*will no longer collect the data for the Admin-C and the Tech-C*" (protective letter, p. 5).

A reason for injunctive relief within the meaning of § 940 ZPO is to be affirmed if there is an objectively founded risk that a change in the status quo could frustrate or impede the applicant's legal enforcement in the future main proceedings (MünchKomm ZPO, § 940 marginal 9).

If the Applicant's request was not granted in the present case, the role of the Admin-C and Tech-C would be effectively abolished by the Defendant. Until there was a decision on the main action, any registrant would be deprived of the option to entrust an Admin-C and/or Tech-C with administering his domain name. This could not be rectified by a decision on the main action with effect for the past. Even if the data was collected in the future, it would not change that up to that date the role of the Admin-C and Tech-C effectively could not be exercised. And, as explained, the Admin-C and Tech-C perform important functions in supporting the registrant in administrative or technical matters and can be held legally liable. If this data is no longer collected, such contact or recourse by law enforcement authorities and possible claimants is practically excluded. Furthermore, there is a considerable risk that other registrars will recklessly follow the Defendant in its view and no longer collect the respective data, even if it is offered. A detailed preliminary assessment by a German court is an important guideline here.

The potential impairments are conceivably small. The Defendant would only be obliged to collect the data lawfully received. A publication of this data (without further explicit consent) is no longer provided for.

If the Applicant were to be referred to the courts in the main action, a decision would not be expected for many years. Moreover, on the basis of the arbitration clause existing in the RAA, it appears questionable whether the main action could be brought before German courts or the ECJ.

A preliminary decision in this regard does not prejudge the substance of the case. The Applicant seeks preliminary injunctive relief. The Defendant would only have to refrain temporarily from selling further domain name registrations in such a way as the Applicant's certified registrar.

The Defendant could also decide to collect data of the Admin-C and Tech-C in accordance with the contractual obligations with reservation until the main action has been ruled upon.

IV. Questions to the ECJ and referral obligation

The Applicant is of the opinion that the present legal questions all are to be decided in the Applicant's favor. With regard to the relevant data protection provisions of the GDPR, there is no known interpretation of the provisions that would lead to the application for a preliminary injunction being rejected.

However, out of legal caution, we refer to the following recital 143 of the GDPR:

“Where a complaint has been rejected or dismissed by a supervisory authority, the Applicant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation.”

If the Senate is therefore convinced that the outcome of this procedure depends on the interpretation of certain provisions of the GDPR, the Senate must refer these possible questions to the ECJ for a preliminary ruling pursuant to Art. 267 TFEU (see 1.). This also applies as an exception in preliminary injunction proceedings. (see 2.).

1. Questions to be referred to the ECJ - conditions for the obligation to refer the case to the Court of Justice

The conditions for submission under Art. 267 TFEU are as follows: The (a) legal questions are relevant to the decision, (b) there is still no case law of the European Court of Justice on these questions, and (c) the application of Union law is not obvious (cf. the conditions in ECJ C 283/81, CILFIT).

a. Relevance for decision

The Applicant is of the opinion that any interpretation of the relevant provisions of Articles 5 and 6 GDPR in the present case must lead to the application for a preliminary injunction being granted on the merits.

The Chamber did not follow this in its initial decision. The Chamber has interpreted relevant questions of the GDPR in a way that is not reflected either in the GDPR or in

previous case law or literature. The Chamber has not examined any relevant regulations. However, if the Senate wishes to maintain this result, it would in any case have to take into account the interpretations of the GDPR set out in the application for a preliminary injunction. If the Senate considers a different interpretation, it would have to refer the question of interpretation to the ECJ if that interpretation were relevant to the decision in the present case.

b. No case law of the ECJ

The GDPR entered into force on 25 May 2018. As far as can be seen, no case law of the European Court of Justice has yet been passed on the issues at hand here.

c. No obviousness

From the Applicant's point of view, the application of Union law is obvious in the sense of her interpretation of the provisions. In particular, it should be noted that the material assessment of the regulation is essentially the same as the previous provisions of the German BDSG. However, if the Senate has doubts in this regard, the Senate should submit questions of interpretation relevant to the decision to the ECJ.

2. The Higher Regional Court of Cologne has to refer even though these are preliminary injunction proceedings

This court would also be obliged to refer to the ECJ in preliminary injunction proceedings.

The Higher Regional Court of Cologne decides in the last instance on the application for a preliminary injunction and is thus specifically entitled to request a preliminary ruling (cf. fundamentally ECJ C-99/00, Lyckeskog).

Admittedly, in cases of preliminary relief, the obligation to make a referral does not normally apply (B. Schima, *Das Vorabentscheidungsverfahren vor dem EuGH*, p. 72 ff.). However, this does not apply if - as here - the main proceedings would be brought before a court that is not entitled to request a preliminary ruling (cf. ECJ C 107/76, Hoffmann-La Roche; BVerfG 2 BvR 2023/06). In the afore cited case, the European Court of Justice set out the guiding principle:

“Article 177(3) of the EEC Treaty must be interpreted as meaning that a national court is not obliged to refer to the Court of Justice a question of interpretation or validity within the meaning of that provision even if the decision taken in the proceedings can no longer be appealed against, provided that each party is free to initiate or request the initiation of a main

action in which the question provisionally decided in the summary proceedings may be re-examined and be the subject of a referral under Article 177.

The obligation to refer the matter to the Court of Justice only lapses pursuant to this judgment if the question can be re-examined in the main case and possibly submitted to the ECJ for a preliminary ruling.

The Federal Constitutional Court has followed this ruling (BVerfG 2 BvR 2023/06, para. 13):

“In proceedings for interim relief, there is in principle no obligation to file for a referral pursuant to Art. 234 para. 3 EC (cf. decision of the Third Chamber of the Second Senate of the Federal Constitutional Court of 29 November 1991 - 2 BvR 1642/91 -, NVwZ 1992, p. 360). Art. 234 para. 3 EC (formerly Art. 177 para. 3 EEC Treaty) must be interpreted, according to the case-law of the ECJ, as meaning that a national court whose decisions can no longer be challenged by appeal under national law is no longer obliged to refer a question of interpretation within the meaning of paragraph 1 of this Article to the Court of Justice if the question arises in a preliminary injunction procedure and the decision to be given is not binding upon the court deciding about the main action provided that each party remains free – also in front of the court of a different branch – to initiate or request initiation of a main action in which the question provisionally decided in the preliminary injunction proceedings may be re-examined and be subject to a referral under Art. 234 EC (ECJ, Judgment of 24 May 1977, Case 107/76 Hoffmann-La Roche/Centrafarm[1977] ECR 957, marginal 6, and Joined Cases 35 and 36/82 Morson and Jhan-jan/Dutch State[1982] ECR 3723, marginal 10).”

Since the relevant contract contains an arbitration clause under which arguably arbitration proceedings would have to be conducted in the United States in the main case, this court is the only one that can refer the above-mentioned questions to the ECJ and must therefore also refer them if it considers these questions to be legally relevant.

In the event of a referral to the ECJ, the Applicant suggests that the Senate should request that the procedure be conducted by means of the expedited procedure pursuant to Art. 105 para. 1 Rules of Procedure of the Court of Justice.

V. On the value in dispute

This procedure and the legal issues raised in the procedure are imminently important for the Applicant. The issue at hand is to maintain a contractual and administrative structure for

domain names, which also provides for the roles of Admin-C and Tech-C. And these roles are very useful - as stated above - for both the registrant and the Applicant, as well as for third parties such as law enforcement agencies and trademark owners.

Furthermore, this decision is of immense importance for the registrar's further dealings with the Applicant and vice versa. The question arises as to whether the parties will continue to find a reasonable consensus solution in a political process with the help of the Temporary Specification and with the involvement of the European Data Protection Committee and all other relevant parties involved, or whether the refusal of individuals to implement in conformity with the RAA and the Temporary Specification will create facts that leave the Applicant no other choice than to take action against this in order to defend the structure developed in a political process.

Against this background, the Applicant appeals to the court to make a detailed decision taking into account all relevant aspects, even if this is a preliminary injunction procedure. If the Chamber or the Senate deems further submissions necessary or relevant, or if an oral hearing is considered helpful, the Applicant will do everything in her power to clarify any remaining questions in writing or at the hearing. In this case, the undersigned politely asks the Chamber and the Senate for a corresponding notification or for a prompt scheduling of the oral hearing.

Dr. Jakob Guhn
Attorney-at-law