RICKERT.NET

fieldfisher

Rickert Rechtsanwaltschaftgesellschaft mbH Kaiserplatz 7-9 53113 Bonn

Regional Court of Bonn
Wilhelmstr. 21
5311 Bonn

Rickert Rechtsanwaltsgesellschaft mbH
Rechtsanwälte
[redacted]
Geschäftsführer
Thomas Rickert
HRB 9269
AG Bonn
[redacted]

WE SERVE FROM ATTORNEY TO ATTORNEY, Sec. 195 ZPO

In advance via facsimile to: [redacted] (35 pages without annexes)

Your reference:
Our reference: 18/178/01/AK

Attorney: Thomas Rickert
Email: [redacted]t

Bonn, July 10, 2018

Docket number 10 O 171/18

In the preliminary injunction proceedings

of the **Internet Corporation For Assigned Names and Numbers**, 12025 Waterfront Drive, Suite 300, Los Angeles, CA 90094-2536, USA

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

- Applicant and Complainant-

vs.

EPAG Domainservices GmbH, [redacted],
represented by their CEO Alexander Schwertner

Attorney of record: Rickert Rechtsanwälte mbH,
Kaiserplatz 7-9, 53113 Bonn

Fieldfisher (Germany) LLP,
[redacted]

- Defendant and Respondent-

fieldfisher

reason: breach of contract

First, we note that the Defendant is now also represented by Fieldfisher (Germany) LLP, in addition to Rickert Rechtsanwaltsgesellschaft mbH by means of a common representation (Sec. 84 ZPO (Civil Procedural Code)). The power of attorney of Fieldfisher (Germany) LLP is attached as

Appendix AG 4.

On behalf of the Defendant we request:

1. **To reject the immediate appeal in its entirety while the decision of the Regional Court Bonn of May 30, 2018, docket number 10 O 171/18, is upheld;**

2. **To reject the application for a preliminary injunction;**

3. **In the alternative, not to decide on application for a preliminary injunction without a prior oral hearing;**

4. **The Applicant bears the costs of the proceedings.**

We agree that, if necessary, to summon for an oral hearing without observing the mandatory notice period.

The court was correct in its decision to reject the Applicant's application. The Applicant's immediate appeal is without merit. Even when considering the reason put forward by the Applicant in its immediate appeal, the Applicant cannot demand from the Defendant to collect the data in question, whereby this likely comprises the collection to enable further transfer of the data. This also applies to the alternative claim.

1. Introductory remarks

The proceeding at hand is the result of the Applicant's inability to assess and adapt its practices to comply with European data protection law.

The Applicant was of the opinion that it could address the concerns expressed by European data protection authorities – which have already existed and been

documented since 2003 – with a few minimal corrections. This is expressly acknowledged in the Applicant's publications on the Temporary Specification:

> *"Consistent with ICANN's stated objective to comply with the GDPR,* ***while maintaining the existing WHOIS system to the greatest extent possible****, the Temporary Specification maintains robust collection of Registration Data (including Registrant, Administrative, and Technical contact information), but restricts most Personal Data to layered/tiered access*" (https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#1; translation by the signatories, emphasis added)

The result is inconsistent, contradictory and ultimately does not comply with applicable law. The GDPR constitutes a paradigm shift and requires more than a few cosmetic changes in publication practice.

The Defendant took the GDPR as an opportunity to review its entire data processing processes. In the course of this review, the Defendant has come to the conclusion that a fundamental restructuring of these processes was necessary, and it is currently in the process of implementing this. The amendments also concern, among other things, the Defendant's collection practice with regard to the data on Admin-C and Tech-C that are the subject of the dispute at hand, and the Defendant has announced that it will no longer collect them after the technical systems have been amended accordingly. The Defendant has also announced this publicly:

> "*In order to have a domain registration system reflective of "data protection by design and default", we started with the GDPR itself and crafted our procedures and policies around it. We built a new registration system with consent management processes, and a data flow that aligns with the GDPR's principles. Throughout the registration life-cycle, we considered things like transparency, accountability, storage limitation, and data minimization.*"(http://www.tucows.com/tucows-statement-on-icann-legal-action/; translation by the signatories).

For the sake of clarification, we would like to point out that domain holders are currently still technically in a position to transmit the data in dispute to the Defendant (however, this is optional for them, and they can also insert placeholders). For technical reasons, it is currently not possible to refuse the acceptance of this data. However, if this data is still transmitted to the Defendant, it no longer

uses it, and employees of the Defendant have no access to this data. The Defendant intends to stop the data collection completely as soon as the necessary technical amendments of the interfaces and IT systems have been completed.

The Defendant's announcements have now prompted the Applicant to take action against the Defendant – apparently because of an alleged risk of first infringement.

In doing so, it attempts to justify the collection of data in dispute with a whole bundle of legal justifications apparently offered as alternatives. The horror scenarios described by the Applicant do not reflect the reality though.

The Defendant's initial practical experience show that it is right with its approach: The Defendant could continue to register domain names, renew registrations and domain names without recourse to the data in dispute, and without impairing the customers. It was also possible not only to accept but also to process submissions from third parties, and in many cases, domain names were suspended because of illegal activities.

Contrary to what the Applicant claims, the Article 29 Working Party has not issued a clean bill of health for the Applicant's modified use of data. On the contrary: the European Data Protection Board - the successor of the Working Group – again delivered an opinion to the Applicant in a letter dated July 5, 2018 – and also referred to the present proceeding. A copy of the letter is handed over as

Appendix AG 5.

In the letter, the Board rejects any attempt to misinterpret the Board's opinions on specific issues as implicit "waving through" data processing;

> *"Needless to say, the issues identified here are without prejudice to additional issues, further inquiries or findings being made by the EDPB or its Members at a later date."* (Appendix AG 5, p. 1; translation by the signatories).

In its letter, the Board expressly points out that the Applicant does not sufficiently distinguish between the Applicant's own and third parties' purposes for processing and that it is not the task of the board, but rather the Applicant is to define retention periods.

The inconsistency of the data protection assessment, which is also evident here, runs like a thread through the Applicant's submission and means that the Defendant cannot fulfil the contractual obligations imposed on it to transfer the data without violating data protection requirements.

Because the Applicant's data processing violates the requirement of purpose limitation pursuant to Art. 5 para. 1 lit. b) GDPR and the requirement of data minimization pursuant to Art. 5 para. 1 lit. c) GDPR (see section 2 below). In addition, the Applicant cannot claim a suitable legal basis (see point 3). In particular, the processing is not necessary for the performance of the contract, as suitable and workable alternatives are available which, if necessary, ensure that the registrant can be reached quickly. Processing on the basis of a legitimate interest is also ruled out: This already follows from the fact that the alleged interests of the Applicant are not sufficiently defined and the Applicant has not weighed them against the conflicting interests of the persons concerned. In any case, however, the Applicant's practice shows that data on Admin-C and Tech-C is not required for the registration and maintenance of a domain.

In addition, the Defendant would, by transferring personal data to the Applicant and third parties who also to have access to the data under the Registrar Accreditation Agreement (RAA), violate Art. 44 et seq. GDPR. Because transferal to parties in countries, which do not have an adequate level of data protection, are only permissible if appropriate transfer safeguards are available. The Applicant, which is based in the USA, is not self-certified under the Privacy Shield Agreement; and the RAA does not provide for the inclusion of standard contractual clauses of the European Union (see section 4).

Furthermore, the Applicant's request cannot be brought in line with the information obligations under Articles 13 and 14 GDPR (more on this in section 5), as the Defendant is not in a position, on the basis of the information made available by the Applicant, to provide the information required by law. In addition, this violates the provisions of Art. 26 and Art. 28 GDPR (more on this in section 6).

The alternative claim is to be rejected in its entirety because, in substance, it amounts to a reduction of invalid provisions to preserve validity that is neither legally nor contractually permissible (section 7). Because the obligation to transfer the data laid down in the RAA applies unconditionally; consent must be obtained. This not only constitutes impermissible coupling (Art. 7 para. 4 GDPR); it is also clear that the Applicant may not, as a "minus" to the main application, request the collection and transmission of data in such cases in which consent is

available. Because the contractual provision constitutes a violation of a legal prohibition, and a qualitative reduction of the provision in order to maintain validity is excluded according to general legal principles. In addition, the severability clause in Clause 7.11 of the RAA provides that invalid provisions shall cease to apply without replacement unless the parties have agreed on an alternative provision.

Moreover, the alternative claim 2 lit. b) is too vague, since the Defendant cannot assess with sufficient certainty whether and which of the data provided by the registrants are personal data.

From a procedural point of view, we point out that the Applicant's request inadmissibly anticipates the main action. In substance, this is an injunction for performance, since the Applicant wishes to ensure that the Defendant provides the data in dispute. Such an injunction for performance is only permissible in exceptional cases; however, the conditions are not met here (see Section 8).

However, the Defendant supports the suggestion that the matter be referred to the ECJ by way of a preliminary ruling. Due to the situation in the present proceedings, this is also possible and necessary in preliminary injunction proceedings (paragraph 9).

In detail:

2. Violation of basic processing principles (Art. 5 GDPR)

The Defendant cannot fulfil the contractual obligation to collect and transfer the data without violating the basic processing requirements laid down in Art. 5 GDPR.

According to Art. 5 para. 1 lit. b) GDPR, personal data must be processed for defined, specified, explicit and legitimate purposes. The purpose of the processing must in principle be determined prior to collection, and the data subjects must be informed of this purpose when collecting the data (see also Art. 13, 14 GDPR). The processing purposes must be clearly defined so that the data subject can foresee the purposes for which the data will be processed and the risks involved (cf. BeckOK DatenschutzR/Schantz DS-GVO Art. 5 marginal 13, 15). In addition, data may only be collected if it is necessary to achieve the purpose (data minimisation requirement). All these requirements are not met by the data processing by the applicant. The defendant may therefore not be obliged to collect the data.

fieldfisher

2.1 Lack of specified purpose

The Applicant has not sufficiently specified the processing purposes for the data of Admin-C and Tech-C:

For the alleged specified purpose, the Applicant first refers to Sections 4.4.5 to 4.4.7 of the Temporary Specification (immediate appeal, p. 11). These are not relevant in this case: Because Section 4.4.7 – the only provision that refers directly to the data in dispute – merely addresses the use of the data on Admin-C and Tech-C for the purpose of publication – which in any case is only possible with the separate consent of the parties concerned:

> *"4.4.7. Enabling the publication of technical and administrative points of contact administering the domain names at the request of the Registered Name Holder;"*

The Applicant's statement that the Temporary Specification clarifies that the purpose of processing is to contact the Admin-C or Tech-C if "*the registrant is unable or unwilling to manage his domain name registration*" (immediate appeal, p. 11) is false. Neither Sec. 4.4.5 nor Sec. 4.4.6 specify any such purpose:

> *"4.4.5. Enabling a mechanism for the communication or notification to the Registered Name Holder of technical issues and/or errors with a Registered Name or any content or resources associated with such a Registered Name;*
>
> *4.4.6. Enabling a mechanism for the Registry Operator or the chosen Registrar to communicate with or notify the Registered Name Holder of commercial or technical changes in the domain in which the Registered Name has been registered;"*

The Temporary Specification therefore does not contain any specific purpose for the use of the data of Admin-C and Tech-C – with the exception of the possibility of publication with the corresponding consent of the persons concerned. The provisions referred to by the Applicant all refer to contacting the Registrant himself.

2.2 Vagueness

Insofar as the Applicant refers to further purposes for processing mentioned in Sections 4.4.8 and 4.4.9 of the Temporary Specification, these are too vague.

fieldfisher

According to these provisions, the Applicant refers to the following purposes of processing:

> *"4.4.8. Supporting a framework to address issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection;*
>
> *4.4.9. Providing a framework to address appropriate law enforcement needs;"*

It remains unclear what "*issues*" should be in connection with the registration of a domain. In addition, the term "*framework*" should be understood here in the sense of a multi-party infrastructure. There is no description of the purposes, the scope of data processing and the identity of the parties involved. This cannot be compensated through 'all-inclusive' and rather buzzword-like references to third-party interests such as consumer protection, cybercrime, DNS misuse, intellectual property protection or "*needs of law enforcement authorities*" – especially as even this list is not exhaustive ("including but not limited to", cf. Section 4.4.8 of the Temporary Specification). In substance, the provisions mentioned by the Applicant are used to legitimize the collection and storage of data for non-specified purposes. This is not permitted (BeckOK DatenschutzR/Schantz DS-GVO Art. 5 marginal 13 with reference to BVerfGE 65, 1 (46)).

In its letter of 5 July 2016, the European Data Protection Board points out once again that the Applicant does not sufficiently distinguish between its own purposes and those of third parties (Appendix AG 5, S.2).

The Board thus shares the view expressed here that the specification of processing purposes is lacking.

2.3 Irrelevance of third party definitions

The contractual terms and conditions of some registrars, also mentioned by the Applicant, which contain only partially congruent, if not conflicting, information regarding the role of Admin-C and Tech-C are also not a suitable specification of the purpose.

According to the sections cited by the Applicant from the contractual conditions of third parties, the Admin-C may act as "*secondary or backup administrator for a domain*", "*should be familiar with plans for the domain name and its use*" or "*be an employee, managing director, manager of the company*". In one case, the role

is described in such a way that "*in case of dispute [...] only the domain holder can override the decisions of the administrator*"; in other case he has "*full authority*". (Quotations see p. 6 *et seq.* of the submission of 13 June 2018).

In accordance with the legal requirements regarding the Applicant's role as data protection (joint) controller it is responsible to define the processing purposes. The Applicant has not fulfilled this task and instead brings forward the role descriptions, which registrars have developed precisely because the Applicant has not made any specifications in this regard. However, there is nowhere a conclusive list of the purposes of use. Nor can the perception individual market participants be relevant. That the Applicant now wants retrospectively conceived task descriptions by third parties to be understood as proof of its own purpose definition within the meaning of Art. 5 (1) lit. b) GDPR, turns things upside down.

2.4 Applicant considers further specification of the purpose necessary

The Applicant also appears to assume that a further specification of the purpose is necessary: On 18 June 2018, the Applicant published the draft of the "*Framework Elements for Unified Access Modell for Continued Access to Full WHOIS Data*" (see https://www.icann.org/en/system/files/files/framework-elements-unified-accessmodel-for-discussion-18jun18-en.pdf). The draft is still open for comment and not adopted. It deals with the conditions under which third parties may be granted access to the full WHOIS data. The first paragraph of the document states that it is to be regarded as a starting point for further discussions with the other parties involved ("*The approach suggested in this paper is a starting place for further discussions with the community*."). The Applicant also considers that the questions as to under what circumstances and for what purposes the data in dispute may be used has not yet been sufficiently clarified.

2.5 No need for data collection for dispute resolution

The Applicant's argument that the collection and provision of the data in dispute is necessary for notification under the UDRP rules (immediate appeal, p. 12) is also incorrect. It is true that in practice, this notification is made; however, the conclusion that this evidences the legality of the purpose for processing is incorrect, since the contractual provisions must comply with the requirements of the GDPR and not every contractual regulation automatically results in legal data processing within the meaning of the GDPR.

Initial experiences in the Defendant's group of companies since 25 May 2018 also show that 25 UDRP proceedings against customers, seven of which were

directed against European registrants, were conducted without any problems and could be handled without any problems in spite of not collecting the Admin-C and Tech-C data.

Evidence: Affidavit of Sara Scruton, Senior Compliance Officer Tucows, Inc, defendant's parent company,
Appendix AG 6.

2.6 Delegation of administrative tasks not necessary

It is also incorrect that without the collection of data on Admin-C and Tech-C it would not be possible for registrants to delegate certain domain management tasks. For this purpose it would be sufficient if the domain holder were allowed to enter a generic e-mail address during registration which would be forwarded to several recipients so that different internal responsibilities of the recipients could be mapped. As far as the Applicant describes the provision of full data on Admin-C and Tech-C as an 'option' and 'added value' for the registrant, this is surprising. The Temporary Specification and the RAA assume that the data must be specified and do not provide for such an option (see section 7 below for details). This is not in conformity with the law with regard to the obligation to design data protection-friendly processes ("Privacy by Design").

2.7 No legitimate processing purpose concerning content control

A legitimate purpose also does not lie in the fact that the indication of the controversial data allows the identification of persons who actually control the registration of the domain name and the respective contents (Immediate Complaint, p. 16). An obligation to control the content of websites for the Tech-C and Admin-C is neither regulated in contracts nor in policies that the Applicant makes part of the contract. In addition, the Applicant's statutes expressly exclude content regulation, Art. 1.1. c of the Bylaws, https://www.icann.org/resources/pages/governance/bylawsen/#article1:

> "*ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide, outside the express scope of Section 1. 1 (a). For the avoidance of doubt; ICANN does not hold any governmentally authorized regulatory authority.*"

Nor do the Applicant's comments in this regard justify the collection of the data in dispute. The accessibility of those responsible for content in the Member States

of the European Union is otherwise regulated by required mandatory legal information (in Germany: § 5 TMG); and the regulations show that also the legislator assumes that a single address available for summoning as well as the possibility for the fast electronic establishment of contact with the provider is sufficient to protect third party rights.

2.8 No necessity for availability check

The Applicant also states the purpose of checking the availability of a domain name. The availability of a domain name can easily be queried without the data in question - and even without knowledge of the domain holder's data. The point is completely irrelevant. Intellectual property rights holders can also contact the registrant in case of abuse and are not dependent on contacting the Admin-C or Tech-C.

2.9 No legitimate purpose due to possible Admin-C liability

The argument that the Admin-C can be liable as a interferer in exceptional cases according to German jurisprudence is also unfounded (immediate complaint, p. 24). A possible liability is no reason for the collection of data. It is not a legitimate interest of the Applicant to provide claimants the largest possible number of defendants. Furthermore, the case law cited by the applicant concerns only the Admin-C, but not the Tech-C and the relevant decision of the BGH (judgment of 9 November 20091 Az. I ZR 150/09) makes clear that the Admin-C has a duty to inspect in special circumstances, the violation of which results in liability for interference. The BGH has expressly rejected a general duty to control which would justify data collection “for retention”.

2.10 No comparability with the role of the representative of a trademark owner

Finally, the Applicant's comparison with the provisions of the trade mark register is not helpful. The databases for trademarks are used – a circumstance which the Court has already correctly pointed out in its decision – based on a legal basis which does not exist in the present case. In addition, domain names and trademarks are not comparable. The trademark owner has an exclusive right against third parties with the consequence that third parties must be able to recognize who has which trademark rights so that trademark infringements can be avoided. Here, however, the purpose is only to make it easier for third parties to assert claims against domain name registrants. It is therefore not justified to derive a legitimate processing purpose from trademark law.

fieldfisher

2.11 Violation of the principle of data minimization, Art. 5 (1) lit. c GDPR

The collection of the data in dispute is also in violation of the principle of data minimization. The collection of data must be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"* (data minimization, cf. Art. 5 para. 1 lit c) GDPR). While the Applicant has mitigated a key problem of the WHOIS service by no longer publishing without restriction the personal data of the registrant, Admin-C and Tech-C, namely the problem that these data are copied and used for spam, phishing, fraud and other illegal activities, this does not go far enough to ensure legal conformity.

As already explained, the collection of contact data for an Admin-C and Tech-C is not necessary to successfully register a domain name, to maintain registration, to transfer a domain name to third parties or, in the event of problems or possible use in breach of contract, to contact and remedy the situation. In light of the principle of data minimization the desired data processing by the applicant is therefore prohibited.

Insofar as the applicant tries to use the numbers produced by the Defendant to try to demonstrate that there is a need for the data collection, because for approximately 5 million domain names there is disparity of the three contact points, the figures actually support the Defendant: it is obvious that the collection Admin-C and Tech-C data is not necessary for the Applicant's tasks, because otherwise it would require these data for the registration of a domain name. The Chamber also correctly points out in its decision (there p. 7), that the three contact points do not necessarily have to be different and that the collection of three data sets was thus not necessary to achieve the purpose. This means that to a considerable extent personal data, which are not necessary, are collected.

The Applicant did not show that the data in dispute is required for the purposes of consumer protection, online fraud investigation, DNS misuse and intellectual property protection (and the defendant denies this). All aspects of the contractual relationship between the registrants and the Defendant can be handled with the data of the account holder and the registrant - including communication in cases of abuse.

The dispensability of additional contact points for the purpose of combating abuse is demonstrated by the following examples of companies and organizations that help their customers combat trademark infringements or product piracy as well as the contractual requirements of the Applicant herself. The Applicant requires the establishment of dedicated contacts with Registries and Registrars, who are

informed by investigators or injured parties or their representatives, as is set forth in Section 3.18 RAA: Accordingly, a registrar must designate an "Abuse Contact" and publish contact details on the registrar's website:

> *"Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse."*

In addition, an "Abuse Point of Contact" must be named, which must be accessible by e-mail and telephone all year around the clock and within 24 hours to respond to abuse reports from law enforcement agencies and consumer protection organizations, among others:

> *"Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law."*

Section 4.1. of Specification 6 of the Registry Agreement – i.e. the contract between the Applicant and the Registries – provides that Registries shall publish an "Abuse Point of Contract" online:

> *"Abuse Contact. Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details."*

Should the Court consider a translation of the contract necessary, please inform us accordingly. The contract is available on the Internet at

fieldfisher

https://newgtlds.icann.org/sites/default/files/agreements/agreement-aiaproved-31 jul17-en.html.

Prima facie Evidence: Specification 6 of the Registry Agreement, Appendix AG 7, available on the Internet at https://newgtlds.icann.org/sites/default/files/agreements/agreement-aiaproved-31 jul17-en.html.

Not least because of the existence of these contacts, security companies usually contact the abuse point of contact at registries and registrars. They usually do not contact Admin-C and Tech-C. Thus, at all companies of the Tucows group, of which the Defendant is a member, since 25 May 2018, 802 instances of phishing were notified. This led to 614 domain domain name suspensions. 172 of these domain names were registered to European Registrants.

Prima facie Evidence: Affidavit of Sara Scruton, **Appendix AG 6.**

The above-mentioned contact points for abuse control show that the collection of Admin-C and Tech-C is not necessary to achieve the purposes stated by the Applicant.

3. No lawfulness of processing, Art. 6 GDPR

The Defendant cannot be obliged to fulfil the contract because the RAA and the Temporary Specification contain clear, but illegal, requirements. It is already wrong to assume that the data collection can be based on alternative legal bases (see below Section 3.1). Furthermore, the Applicant may neither rely on a consent-based collection (more on this under section 3.2) nor on data processing for the fulfilment of a contract (more on this in section 3.3) or on data processing due to legitimate interests (more on this under point 3.4).

3.1. No alternative legal bases

The Applicant argues that the data collection in dispute is permissible based on various legal bases (Immediate Appeal, p. 14: collection of data for contract fulfilment; p. 15: collection of data based on legitimate interests; p. 26: requirement for consent). The view thereby expressed by the Applicant, that the Court should pick and choose the appropriate legal basis, is astonishing, because the GDPR requires that the legal basis is determined before the processing of data begins. A change between individual legal bases, as the Applicant now proposes, is im-

permissible under data protection law and contradicts the transparency requirement. This already follows from the fact that the user is informed about the legal basis of data processing (Art. 13 para. 1 lit. c) GDPR and Art. 14 para. 1 lit. c) GDPR, see on this also BeckOK-DatenschutzR/Schantz DS-GVO Art. 5 para. 10).

The Applicant must let itself be asked what the specific legal basis is - and which requirements, which must be clear, the Applicant is supposed to have stipulated in the Temporary Specification. Already the RAA and the Temporary Specification are contradictory in this respect, because a consent requirement (RAA Section 3.7.7.6) and the processing reason of a legitimate interest (Temporary Specification, Appendix C - Annex AS 7) are being formulated at the same time. An alleged contractual relationship between the registrant and the Admin-C or Tech-C is for the first time established during these proceedings and is not reflected in the contractual basis. In any case, the contractual relationship between the registrant and the registrar shall be decisive for the admissibility of data processing under data protection law, in particular pursuant to Art. 6 para. 1 lit b) GDPR

In detail:

3.2 No collection based on consent

It is not possible to collect the data in dispute on the basis of consent.

3.2.1 Precise requirements in the Temporary Specification

The statutory mandate of the Applicant includes the development of policies for gTLDs. These policies are intended to ensure interoperability between all parties involved in the operation of gTLDs. For example, the fact that a domain name can be carried from one registrar to another is due to the fact that the so-called transfer policy specifies exact specifications that must be observed by all providers. The purpose of the Temporary Specification of the Applicant was that in view of the introduction of the GDPR a uniform approach of the providers is ensured. The goal as understood by the providers and thus also by the Defendant was that the Temporary Specification defines clear legal, organizational and technical specifications.

The Applicant regulates every aspect of data processing in its policies and sanctions non-compliance through its "Contractual Compliance"-Team. Where there are various options for data processing, the Applicant regulates this explicitly.

fieldfisher

However, the optional collection of the data for Admin-C and Tech-C is not provided for, only the optional publication of such data with consent, see sections 7.2.2. and 7.2.4 of the Temporary Specification, Appendix AS 7.

If the Applicant now claims that the Defendant should have exhausted all possibilities of data collection, the Applicant contradicts its own specifications with this demand. The Temporary Specification does not offer flexibility for registrars with respect to Admin-C and Tech-C data.

Accordingly, in its letter of 5 July 2018 (**AG 5**), the European Data Protection Board recommends that the Applicant amend the Temporary Specification in view of the present proceedings. The registrant shall be free to provide either Admin-C and Tech-C data identical to the registrant or to provide non-personal data (e.g. "admin@domain.com"). The Board obviously shares the Defendant's view that the RAA and the Temporary Specification do not at present provide for optional collection of the data in dispute.

Such an optional - and thus consent-based - solution could also not be implemented without further ado (see also Section 3.2.3). Because there is a lack of necessary technical and organizational requirements. This is recognized by the Applicant, who deliberately does not require registrars to distinguish between natural and legal persons (see in detail Section 7.3.2.). In addition, the implementation of a consent based approach requires an industry-wide technical standard with corresponding protocols and shared interfaces to share the consent information to be able to exchange consent information between participants. Such a standard does not yet exist.

Prima facie Evidence: Affidavit in lieu of an oath by Sara Scruton, Senior Compliance Officer Tucows, Inc, Parent Company of the Defendant, **Appendix AG 6**

3.2.2 Unlawful obligation to obtain consent

The Defendant can certainly not be obliged to obtain a mandatory consent. This would violate Art. 7 para. 4 GDPR. According to this provision,

> *"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."*

fieldfisher

The GDPR thus contains a prohibition of coupling - consent must not be required if the data is not necessary to fulfil a contract (and if they are, no consent is usually required, cf. Art. 6 para. 1 lit. b) DSGVO). The person concerned must therefore have the right to use the service or to provide it, without giving consent to – the not absolutely necessary – use of personal data. Stemmer in BeckOK DatenschutzR OSGVO Art. 7 paras. 40-47 states as follows in that regard:

> *"The purpose of the rule supports a restrictive interpretation. It is not sufficient that the data processing is provided for contractually, but it must be absolutely necessary for the actual performance of the owed contractual performance."*

However, the provision of data for Admin-C and Tech-C is presently not required (see para. 2 and para. 3.4 below).

Contrary to the Applicant's view, however, the Applicant does not give the Defendant and the registrants the choice of collecting the data in dispute. According to 3.3.1 RAA, the Defendant is obliged ("shall consist of the following data") to provide the data referred to in 3.3.1.7 and 3.3.1.8 with regard to Admin-C and Tech-C. Similarly, the Applicant does not state that the persons affected are free to give their consent. This is because in 3.7.7.6 RAA, the registrant assures ("represents") that he has received the consent.

In summary, this means that the Defendant is unconditionally obligated by contract to collect the data and that the Defendant must pass on the obligation to the registrants in an equally unconditional form in order to comply with this obligation. These, in turn, have no choice but to demand the consent of the persons who are to act on their behalf as Admin-C or Tech-C, as otherwise they will not be able to fulfil their contractual obligation towards the Defendant. The flexibility claimed by the Applicant in collecting the data does not exist. The Applicant therefore infringes the prohibition of coupling with the RAA.

It is also noteworthy that the Applicant relies on paragraph 3.3.1 RAA to require consent-based data collection. It is precisely this illegal and far too broadly worded consent to the collection and further processing of the data up to their unrestricted publication via the WHOIS service that was supposed to be corrected with the Temporary Specification. In this, the Applicant distinguishes between the collection and publication of the data and assumes that the former can be based on Art. 6 para. 1 lit. b) GDPR (or Art. 6 para. 1 lit. f) GDPR), whereas the latter can only be done with the consent of the data subject. If the Temporary Specification regulates this aspect, it represents the more specific provision and thus

takes precedence over the general - and in any case illegal - general consent requirement of the RAA.

The Applicant may not require the defendant to demand consent of its contracting partners. However, if the Applicant now submits that this very consent is voluntary, it becomes clear only once more that the collection of the data in dispute is not necessary from the Applicant's point of view either: because if the consent is voluntary, then the Applicant must also deal with such cases in which the consent is not granted - and the Applicant does so in at least 50 percent of all cases.

3.2.3 Impossibility of obtaining legally valid consent

Nor may the Defendant be referred to the need to obtain consent to the transfer of data to the Applicant and other interested parties such as Registries for other reasons. This is because the instrument is unsuitable for the present case - in the present case it is not possible to obtain consent in conformity with the law and to comply with the related requirements of the GDPR.

Consent must be "informed" (Art. 7 (1) GDPR in connection with Art. 4 no. 11 GDPR). The general information requirements apply, which also apply to data collection on a statutory basis. In the case of a direct collection, the information from Art. 13 (1) lit. a)-c) and e)-f) (Wolff/Brink in: BeckOK Datenschutzrecht, 24. Edition, DSGVO Art. 7, marginal 55) must be provided. With regard to the obligation to inform about third parties (Art. 13 para. 1 lit. e) GDPR), the probably prevailing view is that contrary to the wording of the provision, there is no alternative between "recipients" and "categories of recipients", but that the recipients are always and the categories of recipients optionally to be named (see Recital 63 GDPR and Wolff/Brink in: BeckOK Data Protection Law, 24th Edition, DSGVO Art. 15, marginal 58). If consent is obtained on this basis, this consequently only includes the recipients named in the consent; if new recipients are added later, consent must be obtained again. It is obvious that consent, which, as in the present case, ultimately concerns transmission to numerous recipients who change over time, is not feasible in practice.

The GDPR also requires that consent by the person responsible can be proven (Art. 7 (1) GDPR). This means that the Defendant would not only have to demand this proof from the domain owners; it would also have to be able to transmit this proof to all other recipients of the data, insofar as they are to be regarded as controllers within the meaning of the GDPR. The Applicant does not currently offer any technical options to submit this proof.

fieldfisher

Finally, the Applicant's assertions on p. 5 of the immediate complaint concerning the Defendant's position and statements in the eco GDPR Domain Industry Playbook (Annex **AS 9**) are inaccurate and out of context. It is correct that they point out risks in connection with consent-based processing of personal data. The requirements set by the Applicant, which must be complied with industry-wide, should be based on legally compliant and reliably collected data. The consent-based data collection is expressly described in the "Playbook" as a possibility of data processing: "*Such data processes are always possible in case a valid consent as required by GDPR is collected from the data subject*" (p. 53). The eco GDPR Domain Industry Playbook, which was created in cooperation with three professionals from Fieldfisher (Germany) LLP and Rickert Rechtsanwaltsgesellschaft mbH, points out risks in the area of proof, the prohibition of coupling and the fact that a given consent can be revoked at any time without giving reasons in accordance with Art. 7 (3) GDPR. Contrary to the Applicant's assertion, this certainly describes risks of both legal and actual nature.

3.3 Data processing for the execution of a contract

We refer to the above and the previous presentation. The collection of Admin-C and Tech-C data is not necessary to fulfill the agreement between the Registrar and the Registrant. The fact that in individual cases there may be a contract between the Registrant and third parties for the provision of the Admin-C or Tech-C is irrelevant for the present consideration.

3.4 Data processing for the protection of legitimate interests

The collection and transmission of data is also not permitted on the basis of legitimate interests. The alleged interests designated by the Applicant (immediate complaint, p. 29) are disputed and the Applicant has not weighed the interests.

For in the context of Art. 6 (1) lit. f) GDPR it must first be determined whose alleged legitimate interests are affected and what they consist of. It is also necessary to explain why data processing is necessary to protect this legitimate interest. We have extensively explained that the processing of the data of the Admin-C and Tech-C is not necessary for the purposes claimed by the Applicant. Even if one wanted to follow the opinion that a data collection would be necessary, the Applicant does not explain why name, address, e-mail address, telephone number and fax number should be collected, if nevertheless only an establishment of contact by anonymized e-mail address or web form is intended and thus at most the collection of the e-mail address would be legitimized – assuming the general necessity of an establishment of contact in the alternative.

fieldfisher

Finally, the Applicant fails to deal with the interests of the persons concerned ("*no doubt*", immediate complaint, p. 22). The Applicant makes it far too easy for itself: because those concerned may well have an interest in ensuring that their personal data are not transferred to other - unknown - parties, some of them outside of the EU, and used for purposes that are not clearly defined. Not all domain names are used for the publication of websites, and not all domains are used commercially. In addition, there are - especially in today's times - quite tangible risks. To describe a not at all absurd scenario: One of the many autocratically governed states has no recourse against a registrant and puts pressure on the Admin-C of a website to prevent the publication of regime-critical information. Such considerations do not seem to play a role for the Applicant in the balancing of interests, but would be necessary for the balancing of interests which is required in order to render the data processing legal.

In this context, it should also be noted that the 'retention' of contact data for many of the processing purposes used by the Applicant must be regulated by law; this applies in particular where criminal prosecution or other sovereign interests are involved. In its ruling on data retention, the European Court of Justice clarified that access to data retained in storage requires prior control by a court or an independent administrative body, and - insofar in principle - confirmed that data processing must always be subject to precise, objective and material conditions. In particular, the ECJ pointed out that all these conditions must be such as to limit the scope of the measure and consequently the scope of the persons concerned (ECJ, Case C-203/151 ZUM 2017, p. 4141, paragraph 103, 110, 120 - Tele2 Sverige AB LJ. a./Post- och telestyrelsen and others). The Defendant does not disregard the fact that the retention of telecommunications data constitutes a far more serious encroachment on the fundamental rights of those concerned than the storage of data here present. Nevertheless, the same applies here: retention and transmission must be proportionate and limited to what is necessary. In the present case, it is not apparent that the Applicant has even weighed up the interests of the persons concerned and has examined less drastic measures to achieve the objectives which it may have pursued. The reference to "*no doubt*" in any case does not do justice to the Applicant's responsibility for the examination.

4. No transfer protection

A number of parties are involved in the registration and further operation of gTLDs, all of whom receive or have access to personal data in accordance with the Applicant's instructions. These are:

fieldfisher

- Registries that operate the central database of all domain registrations in the TLD they manage and make it available via the "Domain Name System;
- Registrars who enable end customers to register domains;
- Possibly Resellers of Registrars;
- The Applicant;
- Escrow Agents for Registries, who regularly store data from the Registry;
- Escrow Agents for Registrars who regularly store data of the Registrar; as well as
- Emergency Backend Operators (EBERO), who take over the technical operation of a Registry in the event of a crisis.

In many cases, the above-mentioned parties are based outside the EU. With the exception of any EU standard clauses or Privacy Shield self-certifications agreed on the personal initiative of the respective operator, there are no transfer protection regulations specified by the Applicant. Although the applicant imposes an obligation on the Registrars to provide appropriate transfer protection, it does not participate in the Privacy Shield itself and has not concluded any corresponding agreements with Registries, Registrars or other third party recipients as far as can be seen.

Even if the Chamber decided to follow the Applicant to the extent that a legal basis for the collection and transmission of the data is in principle possible and that the provision of the RAA in dispute is unobjectionable, an order can only take place step by step (*Zug-um-Zug*) in exchange to the conclusion of a transfer protection which is in accordance with the legal requirements. No contract has yet been concluded between the Parties on the basis of the standard contractual clauses. In this context, it should also be noted that these requirements must also be observed with regard to any further transmission by the Applicant to third parties, as provided for in the RAA (Art. 44 sentence 1, second half of the sentence of the GDPR). As far as the Defendant is aware, the Applicant has not yet taken any measures to comply with the relevant obligations formulated by itself (cf. Temporary Specification, Appendix C, Section 3.10).

Already for this reason the data processing, which in the case of the Applicant consists of access to data for compliance purposes, is without legal basis.

fieldfisher

5. Incompatibility with the information requirements of Art. 13 and 14 GDPR

The Applicant may also not require the Defendant to collect and transmit data because, on the basis of the information provided by the Applicant, the Defendant is not in a position to fulfil its duty to inform registrants and thus indirectly the data subjects. Art. 13 GDPR prescribes that the data subjects are informed at the time the data are collected. This obligation to provide information covers not only the purposes of the collection, but also the specific legal basis. The recipients or categories of recipients must also be named. On none of the above points could the Defendant provide sufficiently specific information on the basis of the information provided by the Applicant. For there is neither a sufficiently specific description of the processing purposes, nor does the Defendant know on which of the many legal bases mentioned by the Applicant data processing is now to be based. Finally, the Defendant is also not in a position to name the third party recipients. The Applicant does not leave it here with a possible information of users, about which according to Sec. 32 para. 1 no. 5 and para. 2 s. 3 Federal Data Protection Act (new) it would not have to provide information, but demands the surrender of data to currently not yet determined third parties on a global level. This makes it impossible for the data subject to be informed in accordance with the legal requirements and prevents the Defendant from feeding data into a system in which it is completely unclear under which conditions which data can be accessed by which persons.

Against the background of this uncertainty and the associated lack of possibility of adequately informing those affected, the collection of data from Admin-C and Tech-C is prohibited.

6. Violation of the requirements of Art. 26 and Art. 28 GDPR

In addition to the requirement of a legal basis for the collection of the data, the disclosure of the data to third parties would also have to be legitimized. The legal requirements for this are lacking for various reasons.

The Applicant derives the claim asserted from the RAA in conjunction with the Temporary Specification. However, there are no provisions here that meet the requirements of Articles 26 and 28 GDPR. A graphical representation of the data flows between the parties can be found on page 8 of the *eco GDPR Domain Industry Playbook* already introduced by the Applicant in the process as Annex **AS 9**. On p. 21 of the Temporary Specification, the Applicant specifies the responsibilities of the parties.

fieldfisher

gTLD Processing Activity	Registrar Role/ Legal Justification	Registry Operator Role / Legal Justification	ICANN Role / Legal Justification
Collection of registration data from Registered Name Holder	Controller (Consent and Performance of a Contract)	Controller (Legitimate Interest and Performance of a Contract)	Controller (Legitimate Interest)
Transfer of registration data from Registrar to Registry Operator or Registry Operator Backend Service Provider	Processor (Performance of a Contract)	Controller (Legitimate Interests)	Controller (Legitimate Interests)
Transfer of registration data from Registry Operator to Data Escrow Agent	No role	Processor (Performance of a Contract)	Controller (Legitimate Interest)
Transfer of registration data from Registrar to Data Escrow Agent	Processor (Performance of Contract)	No role	Controller (Legitimate Interest)
Transfer of registration data to ICANN Contractual Compliance	Processor	Processor	Controller (Legitimate Interest)
Transfer of registration data to Emergency Backend	No role	Processor (Performance of a Contract)	Controller (Legitimate Interest)

fieldfisher

gTLD Processing Activity	Registrar Role/ Legal Justification	Registry Operator Role / Legal Justification	ICANN Role / Legal Justification
Registry Operator (EBERO)			
Public RDDS/WHOIS	Controller (Legitimate Interest)	Controller (Legitimate Interest)	Controller (Legitimate Interest)
Disclosure of non public RDDS/WHOIS to third parties	Controller (Performance of a Contract [can also vary depending upon the requesting party])	Controller (Performance of a Contract [can also vary depending upon the requesting party])	Controller (Performance of a Contract)
Data retention	No role	Processor (Performance of a Contract)	Controller (Performance of a Contract)

But for in exceptional cases where Registries and Registrars have concluded agreements on their own initiative, the Applicant has not yet concluded or even only offered any order processing agreements between the parties pursuant to Art. 28 GDPR or joint controller agreements pursuant to Art. 26 GDPR, although Registries, Registrars and the Applicant are named as controllers in the second line. In its letter of 6 December 2017, the Article 29 working group indicated that it might assume that Registries together with the Applicant are joint controllers under Article 26 GDPR. In addition, for the tasks of the Escrow Agent, the Registries are named as processor and the Applicant is named as controller.

Prima facie evidence: Letter of Art. 29 AG dated 06 December 2017,

Annex AG 8

The Applicant has not yet concluded any or sufficient order processing agreements in the constellations where it engages contract processors, and has not yet submitted a joint controller agreement where it becomes active alongside other controllers. Even if the Applicant did not wish to assume the role of joint data controller, it is unclear how the Applicant explains why it wishes to have access to data, specifies the handling of all data meticulously and also takes legal action by means of infringement proceedings or - in the present case – court proceedings. Agreements to this effect are apparently currently being developed.

fieldfisher

There is no (a) legitimization of the transfer of data requested by the applicant for registrants, Admin-C and Tech-C to the respective Registries; (b) legitimization of the transfer of data to the Escrow Agents; (c) legitimization of the transfer to the EBERO; and (d) legitimization of the transfer of data to the Applicant.

The Data Processing Agreement recently submitted by the Applicant to the Registries, presented here as a

Annex AG 9,

does not change anything. It concerns only the relationship between Registries and Registrars, and it does not contain a sufficient purpose either.

7. Alternative claim

The Applicant's alternative claim, which has now been lodged for the first time with the immediate appeal, is also unfounded. Section 3.4.1 of the RAA cannot be interpreted in a valid manner (*geltungserhaltend*) as meaning that the Defendant would be obliged to collect the data only to the extent that consent has been given or the data is not personal. The alternative claim is also unspecific.

7.1. Invalidity of Sections 3.3.1.7 and 3.3.1.8 RAA

In its decision of 29 May 2018, the Bonn Regional Court correctly assumes that the Defendant does not have to comply with Section 3.4.1 in connection with Sections 3.3.1.7 and 3.3.1.8 RAA. According to Art. 6(1) GDPR, the processing of personal data is lawful only if at least one of the permissions of this article is fulfilled. This is presently not the case. By collecting the data required by the contract, the Defendant would violate applicable data protection law (see numbers 2 - 5 above). The contractual obligation to collect personal data despite a lacking legal basis thus constitutes a violation of a prohibition law (*Verbotsgesetz*, Sec. 134 BGB).

However, the prohibition of the collection of certain personal data at issue here does not result in the total invalidity of the contract concluded between the parties to the dispute, but merely leads to the invalidity of Sections 3.3.1.7 and 3.3.1.8 of the RAA. For the parties have agreed in Section 7.11 RAA that if a clause of the RAA is invalid and no agreement can be reached on a replacement of the clause concerned, the remaining parts of the contract shall remain intact:

fieldfisher

> *"If one or more provisions of this Agreement are held to be unenforceable under applicable law, the parties agree to renegotiate such provision in good faith. In the event that the parties cannot reach a mutually agreeable and enforceable replacement for such provision, then (a) such provision shall be excluded from this Agreement; (b) the balance of this Agreement shall be interpreted as if such provision were so excluded; and (c)* ***the balance of this Agreement shall be enforceable in accordance with its terms****."* (Emphasis by the undersigned)

Notwithstanding this, the total invalidity of a legal transaction foreseen in § 134 BGB would only kick in, if an interpretation of the prohibition law (*Verbotsgesetz*) leads to the conclusion that the legal transaction is not to become effective according to the meaning and purpose of the prohibition (BGH, NJW 2003, 3692)" (BGH, judgment of 25.09.2015 - IX ZR 25/14 = NJW 2014, 3568 Rz. 14). Decisive for the assessment of the purpose of the respective prohibition standard is whether the law itself wants to prevent economic performance (BGH, judgment of 22.12.2000 - VII ZR 310/99 = NJW 2001, 818, (819)). The GDPR begins by clarifying its subject matter and the objectives it pursues:

> *"This Regulation lays down* ***rules relating to the protection of natural persons with regard to the processing of personal data*** *and rules relating to the free movement of personal data."* (Art. 1(1) GDPR; emphasis by the undersigned).

The purpose of the GDPR is therefore, in order to protect the personal rights of natural persons, to prevent certain data processing operations described by the provisions of the Regulation or to authorize them only under certain conditions. According to a purposeful interpretation, it can therefore only be assumed in this case that the clauses obliging the Defendant to unlawfully process data are merely partially invalid. The collection of administrative and technical contact data concerns only a marginal aspect of the cooperation of the parties in domain registration. It is therefore to be assumed that they would have concluded the contract even without the void part, § 139 BGB.

7.2 No reduction to preserve validity

However, an interpretation preserving validity (*geltungserhaltende Auslegung*) of the aforementioned clauses is ruled out for both legal and contractual reasons. The Applicant may not require the Defendant to collect the data in any event if consent has been obtained or the data are not personal (alternative claim 2).

fieldfisher

An interpretation preserving validity of contractual clauses is only permissible under strict conditions according to highest court rulings. These are not given here: The case-law only recognizes the possibility of an interpretation preserving validity in cases where the clause concerned is quantitatively divisible (e.g. beer supply contracts with an excessively long commitment, excessively long non-compete obligations). The Federal Supreme Court has repeatedly stated that a qualitative reduction is out of the question:

> *"Despite the replacement clause provided for under V of the subcontractor agreement, the non-compete clause agreed here does not permit a valid reduction to an admissible customer protection clause.* ***This would require a change in the objective limits of the ban. That is out of the question. Only if the non-compete obligation exceeds the permissible time limit is a reduction to the extent still to be approved possible*** *(cf. BGH, NJW 2005, 3061[3062]; WM 2000, 1496[1498]; WM 1997, 1707[1708]).”* (BGH, judgment of 10 December 2008, ref. KZR 54/08, GRUR 2009, 698 (marginal 25); emphasis by the undersigned)

Nor does the protection of legitimate expectations justify any other assessment. Because it is not the case that the controversial data collection only became illegal with the entry into force of the GDPR and was previously legal. The Applicant has been aware for more than 10 years that the WHOIS practice is subject to significant concerns from the European data protection authorities and the Applicant has not managed to resolve these concerns during this time by adapting its structures and contracts.

However, protection of legitimate expectations is also not necessary for another reason: After all, the Applicant has specifically reacted to the legal framework changed by the GDPR with the Temporary Specification. It has - wrongly - not seen any need for change with regard to the data collection practice which is subject of the dispute here. In principle, however, it was possible to use the Temporary Specification to standardize a change in the data collection practice in dispute. The Applicant did not do so. It would be inequitable to pass these omissions on to the Defendant by means of an interpretation of the contract that would preserve the validity *"to a degree permissible under data protection law"*. It is in the Applicant's own hands to reduce the obligations to collect personal data to a level that complies with data protection regulations by adjusting the contractual basis.

If one were to allow an interpretation preserving validity, the data protection risk would be completely passed on to the Defendant despite the Applicant's power

over processes and the drafting of contracts. In addition, the Applicant has so far failed to describe the purposes of data processing, the data specifically required for this and the legitimate interests in a manner that might potentially be subsumed (*subsumiert*) under the statutory provisions (see section 3.4). Furthermore, the Applicant does not offer suitable protection for international data transfer, either with regard to the transmission to itself or to other third parties required by the RAA, see section 6 above.

Ultimately, however, the question of the legal admissibility of an interpretation preserving validity is irrelevant: Because the parties have agreed in Clause 7.11 RAA that if a clause of the RAA is invalid and no agreement can be reached on a replacement of the clause concerned, the entire clause is excluded (see section 7.1 above). The Applicant cannot therefore rely on an interpretation of the provisions of the RAA which are the subject of the dispute must be made within the framework of what is legally permissible.

7.3 Insufficient specificity of the alternative request 2.b)

The alternative motion under 2.b) is inadmissible for lack of speficity. With the alternative claim, the Applicant restricts the requested obligation to collect data to the effect that the Defendant should only collect data if it is not personal data. The defendant cannot determine with certainty whether a personal reference exists.

7.3.1 Factual impossibility of differentiation

According to Art. 4(1) GDPR personal data is "*any information relating to an identified **or identifiable** natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" (emphasis by the undersigned). It is important that the question of identifiability does not depend solely on the Defendant's existing knowledge: According to recital 26 GDPR, when determining whether a natural person is identifiable, "*account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller **or by another person** to identify the natural person directly or indirectly*" (emphasis by the undersigned).

The Defendant cannot therefore reliably assess whether or not a data is personal, since it cannot know what further knowledge may be available to the Applicant or

other third party recipients that might enable identification. For example, a telephone or fax number may not be personal to the Defendant; however, the Defendant cannot know whether this telephone or fax number is assigned to a specific employee on the domain holder's side. This also applies to generic e-mail addresses (such as info@icann.com), which, if assigned to a specific person in the organization's internal assignment plan, would be considered personal data. This becomes even more obvious if an e-mail address is not obviously generic, such as reg@domain.com - the Defendant cannot know whether the address is assigned to the "Registration" function or to a person named "Reginald".

The Defendant could therefore not comply with the prohibition as ordered with sufficient certainty, and a corresponding order would shift the substantive legal dispute to the enforcement stage.

7.3.2 Clarity of the contractual provisions

The Applicant may not, for other reasons, succeed with the alternative claim.

The Applicant made the collection of the data elements in dispute mandatory and was aware of the scope of the specifications made. In connection with the collection of registrant data, there has been a public debate on whether registrars should distinguish between natural and legal persons when collecting data. This very point is described in the appendix to the Temporary Specification "*Important issues for further Community Action*" as an ongoing discussion point *("[...] the ICANN Board encourages the community to continue discussing* so *that they may be resolved as quickly* as *possible after the effective date of the Temporary Specification. [...] (5) Distinguishing between legal and natural persons to allow for public access to the Registration Data of legal persons, which are not in the remit of the GDPR").*

This discussion was motivated not least by the desire to publish as much data as possible. Since the GDPR only protects personal data, some of the parties involved wanted to exclude company data from "protection against publication" within the framework of WHOIS. The Applicant did not accept this request: it expressly did not require registrars to distinguish between natural and legal persons, since registries and registrars had pointed out that a company name of legal person, for example, may also have personal references, so that a distinction between natural and legal persons does not ensure the legality of data processing, is risky and it is also technically impossible to make such a distinction with certainty.

Finally, the data format specified by the Applicant does not provide for any differentiation between natural and legal persons. It is incomprehensible why, in the case of registrant data, the Applicant expressly does not expect registrars to differentiate between natural and legal persons, but in this case demands that they do so.

8. No reason for preliminary injunction

Moreover, the applications for a preliminary injunction are inadmissible because they preempt the main action. The prohibition requested by the Applicant to offer domains without collecting the data in dispute is an order for performance: The Applicant demands compliance with the RAA, i.e. the collection of the data in dispute. The Applicant's astonishing view that the Defendant could temporarily suspend the sale of domains does not change this (immediate appeal, p. 35). Of course, almost any prohibition order can be complied with by completely discontinuing business operations. However, if this were the only way to comply with the required prohibition, the necessary balance (see below) would of course also be in favor of the Defendant.

After all, an injunction ordering performance may only be issued under strict requirements that are not met here: Firstly, the claimant must urgently need the immediate fulfilment of the claim; secondly, it is necessary that the conduct of the main action is not reasonably possible because performance must be effected urgently in order not to lose its meaning; and thirdly, the disadvantages for the creditor must not only be severe but must be disproportionate to the disadvantages of the debtor. According to these principles, it is in any case necessary that when weighing the interests of the creditor against the interests of the debtor, the interests of the creditor clearly predominate because the enforcement of the claim is particularly urgent for the creditor because of the risk of further impairments of his claim and, on the other hand, the risk of the debtor being unjustly obliged in the injunction proceedings is relatively low (BGH, decision of 11 October 2017, docket no. I ZB 96/16, WM 2018, 332).

At least two of these conditions are not fulfilled: Neither does the Applicant need the data urgently; this is shown by the fact that in 50 percent of cases domain holders do not provide separate data for the Admin-C and Tech-C, and yet the Applicant is not prevented from administering and maintaining the domains of these domain holders. Also, there are no significant disadvantages for the Applicant if the data is not made available (see sections 2 and 3 above).

fieldfisher

At the same time, there are considerable risks for the Defendant, in particular in the form of high fines in the event of illegal data processing established by a supervisory authority. There is no doubt about this:

(a) The Applicant cannot rely on a legitimate interest for the collection and processing of the data in dispute (see in more detail under sections 2 and 3.4).

(b) The Defendant would violate the prohibition to transfer personal data to a non-EU country by transmitting the data to the Applicant because no transfer protection measures (such as standard contractual clauses of the EU Commission, self-certification according to Privacy Shield) were taken between the parties (see section 4);

(c) The Applicant cannot refer the Defendant to consent (see section 5).

In addition, there are considerable risks for those affected by the data processing (see Section 3.4).

It must be conceded to the Applicant that in the present case main proceedings because of a referral to the European Court of Justice, which would possibly only be brought about after exhaustion of the legal recourse, would not be helpful for a rapid clarification of the legal question here due to the necessity of a (see also section 9).

9. Referral to the ECJ

The Defendant shares the view that the present court is obliged to refer the matter to the ECJ if and insofar the present court is of the opinion that provisions of the GDPR are relevant to the decision.

9.1 Relevance of decision and notoriety

In essence, the proceedings concern the interpretation of the provisions of the GDPR, which only came into force on 25 May 2018. There is neither a consolidated case law nor a clear line of interpretation for the relevant provisions of Art. 6 GDPR and the requirements of Art. 5 GDPR. This applies in particular to the interpretation of the elements of fact "legitimate interest", "necessity" and the question to what extent legitimate interests of third parties can be weighed against the rights and interests of the registrants concerned and their auxiliary

persons and when they may even outweigh them. According to the relevant CIL-FIT doctrine, there is an obligation for referral for the court, since its decision can no longer be appealed and there is neither an *acte clair* nor an *acte éclairé* situation: The ECJ has not yet ruled on the issues in dispute here, and the legal situation is not so clear that there are no reasonable doubts about the ECJ's position.

9.2 Referral obligation also in preliminary injunction proceedings

The Defendant acknowledges that a referral to the European Court of Justice in preliminary injunction proceedings is generally out of the question. However, the circumstances justify an exception:

(a) The Defendant may not be referred to the conduct of the main proceedings. It is thus the case provided for in Article 287 TFEU that the decision of the present court "*cannot be contested by appeal under national law*". This is because the RAA contains an arbitration clause according to which arbitration proceedings are mainly to be conducted in the USA. In the case of a preliminary injunction, a request to the Applicant to bring a main action (Section 926 German Civil Procedural Code *(ZPO)*) with the aim of referring the matter to the European Court of Justice would come to nothing, since it can be assumed that in this case the Applicant would refuse an amicable cancellation of the arbitration clause.

This is not contradicted by the case law of the European Court of Justice or the Federal Constitutional Court. The courts have made it clear that there is no obligation for referral in preliminary injunction proceedings only ***"provided that each of the parties is entitled*** *to institute proceedings or to require proceedings to be instituted on the substance of the case and that during such proceedings the questions provisionally deveded in the summary proceedings may be re-examined and may be the subject of a reference to the court under Article 177"* (ECJ docket No: C-107/76, 2nd guiding principle - Hoffmann-La Roche; BVerfG docket No: 2 BvR 2023/06, paragraph 13; emphasis added). This is not the case here, as shown.

(b) A referral is also required for other reasons: Under the EU Treaties, the judicial interpretation of European Union acts takes place in a system of cooperation between national courts on the one hand and the European Court of Justice on the other. In this system, the ECJ alone is responsible for ensuring legal unity, i.e. ensuring a uniform interpretation of Union

acts. With regard to the importance of the referral proceedings, the ECJ stressed:

> *"Article 177 [today: Article 267 TFEU] is essential for the preservation of the community character of the law established by the treaty and has the object of ensuring that in all circumstances this law is the same in all states of the community." (*ECJ C-166/73, margin 2 – Rheinmühlen/Einfuhr- und Vorratsstelle Getreide*).*

In the decision of *the* ECJ already cited by the Applicant it further states:

> "*Article 177 (now Article 267 TFEU) whose purpose is to ensure that community law is interpreted and applied in a uniform manner in all the member states, the particular objective of the third paragraphs is to prevent a body of national case-law not in accord with the rules of community law from coming into existence in any member state." (ECJ docket No: C-107/76, margin 5 - Hoffmann-La Roche).*

The uniform application of the relevant provisions of the GDPR would be seriously jeopardized without a referral to the European Court of Justice. Through its contractual conditions, the Applicant dictates both the collection and handling of personal data worldwide. Given the considerable risks to which they are exposed in the event of breaches of the General Data Protection Regulation (the General Data Protection Regulation contains a sanction framework of up to € 20,000,000 or 4% of annual worldwide turnover), similar legal disputes are imminent in all Member States of the European Union. An inconsistent interpretation of the provisions of the General Data Protection Regulation by national courts would have devastating consequences for the entire domain industry. In the event of divergent national decisions, no one would ultimately know which data processing operations should be carried out in accordance with the General Data Protection Regulation.

(c) Also the the *effet utile* doctrine requires a referral. The European Court of Justice has repeatedly stressed that the interpretation of Community law must focus in particular on its practical effectiveness. By this the Court of Justice means an interpretation which seeks to give effect to the objectives pursued by a legal provision of Community law in the most effective manner (cf. Callies/Ruffert, EUV/AEUV 5, Edition 2016, Art. 19 TEU, cf. paragraph 16 m.w.N.). Also against this background, an interpretation of Art. 267 (3) TFEU based on the uniform interpretation of Community law

fieldfisher

is mandatory. Otherwise, the interpretation of the GDPR would be left to an US arbitration court.

The Defendant also agrees with the Applicant's suggestion that, in the event of referral to the ECJ, a request be made for an expedited procedure pursuant to Art. 105 para. 1 VfO-EuGH.

9.3 Alternatively: Obligation to refer to the ECJ to clarify the obligation to refer in the context of interim injunction proceedings

In the alternative, we would point out that - should the court have doubts about its obligation to refer pursuant to Art. 267 (3) TFEU – also in this regard a question to be decided by the ECJ itself would arise. After all, it is ultimately a question of EU law whether a referral under Art. 267 para. 3 TFEU is in principle ruled out in preliminary injunction proceedings.

In the Defendant's view, the ECJ has already answered this question to the effect that there is no obligation to file a preliminary injunction only if both parties are free to instigate main proceedings. (ECJ docket no. C-107/76, 2nd ruling - Hoffmann-La Roche*).* This is presently not the case, since the party defeated in these proceedings is dependent on the cooperation of the other party in order to lift the obligation to arbitrate by way of an amendment to the contract. This might amount to an *acte éclairé*.

If the present court does not follow this view, it is obliged to make a referral in accordance with the criteria of the CILFIT doctrine. Because, apart from the case law of the European Court of Justice cited above, there is no decision on the decisive question here as to whether a referral in preliminary injunction proceedings is in principle excluded even if main proceedings cannot be instigated, and it cannot be assumed either that there are no reasonable doubts that the European Court of Justice in principle wishes to exclude a referral in preliminary injunction proceedings in these cases.

Against this background, we propose the following question for referral:

> *"Must Art. 267 par. 3 TFEU interpreted to the effect that a national court is in a preliminary injunction proceedings obliged to refer a question of interpretation in the sense of Art. 267 par. 1 TFEU to the Court of Justice where the decision taken in the injunction proceedings can no longer be appealed against and the losing party to the dispute on the basis of an arbitration clause, which refers the dispute to an arbitral tribunal outside*

fieldfisher

the European Union, has no possibility, without the cooperation of the other party, to initiate or have initiated itself main proceedings in which the question provisionally decided in the summary proceedings may be re-examined and be the subject of a referral under Article 267 TFEU.

We ask for a decision in accordance with our requests.

Thomas Rickert
Attorney at law
Rickert Rechtsanwaltsgesellschaft mbH

[redacted]
Attorney at law
Fieldfisher (Germany) LLP