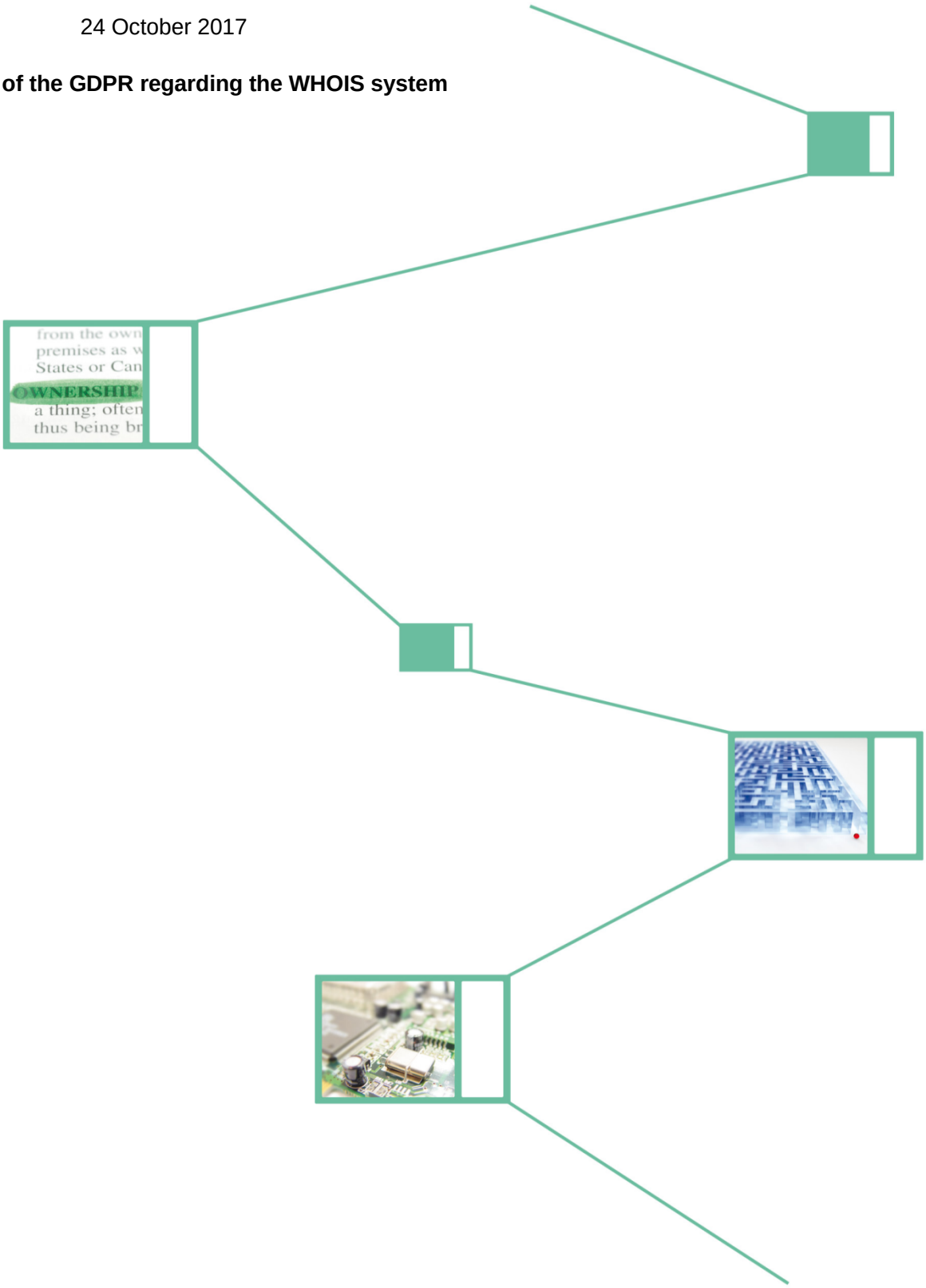
Matter: **ICANN/IPC - 6007313/17 - ICA3.D1000**

From: Paul Voigt, Fritz-Ulli Pieper, Taylor Wessing

To: Intellectual Property Constituency

Date: 24 October 2017

Impact of the GDPR regarding the WHOIS system



TaylorWessing

Executive Summary

- **With regard to the data processing involved with the WHOIS search, relying on registrants' consent as set out in the current form will bear relevant compliance risks under the GDPR. However, these risks may be reduced by implementing measures to ensure that consent is freely given, e.g. by strengthening voluntary privacy or proxy services, formal requirements and documentation procedures.**
- **Even without consent, the data processing in question may be lawful under Art. 6 (1) 1 lit. f GDPR ("legitimate interest" provision), especially if additional measures are taken to safeguard the privacy rights of the registrants, such as privacy or proxy services, captchas etc.**

I. Introduction

1 The Intellectual Property Constituency ("**IPC**") is currently investigating the impact deriving from the General Data Protection Regulation ("**GDPR**") and the potential changes required within the organizational processes of the Internet Corporation for Assigned Names and Numbers ("**ICANN**"). Particularly, IPC seeks advice on the impact of the GDPR upon the obligations of registrars and registries to obtain and input user data into the WHOIS system for publication to internet users. Different questions as to the compatibility of the existing WHOIS system with the GDPR have been raised, with a focus on two main areas of concern. In that regard, IPC has asked Taylor Wessing Partnerschaftsgesellschaft mbB ("**Taylor Wessing**") for its opinion on questions involving matters of consent and legitimate interests. This memorandum shall answer these questions.

II. Facts of the case

2 ICANN coordinates the allocation of unique names and addresses on the Internet. This includes the coordination of the domain name system and the allocation of IP addresses. Particularly, ICANN coordinates all existing internet addresses and ensures that each domain exists only once and is clearly identifiable and accessible via the web browser. ICANN is not actively involved in admission and registry of these addresses. In fact, generic top-level domains ("**gTLD**") registrations are administered by authorized ICANN contracted partners: registries and, subsequently, registrars, providing registration services to registrants. A registrant (individuals, businesses, or-

ganizations or governments) can register a domain name directly with a registrar (or through a reseller that has a relationship with a registrar). The registrar works together with the registry, which is the entity that maintains the authoritative record of all registrations for the gTLD, i.e. the authoritative database for the domain names.

3 Registrar and registry services include the operation of WHOIS-Servers in order to provide information services to internet users. ICANN requires ICANN accredited registrars and registries to implement WHOIS services and comply with technical specifications for the WHOIS services offered by them, as described in ICANN's contracts with registrars and registries. The ICANN 2013 Registrar Accreditation Agreement (RAA) sets out comprehensive obligations which are binding on all gTLD domain name registrars. It has to be noted that country code top-level domains ("**ccTLDs**") are not subject to any ICANN requirements regarding WHOIS services. Furthermore, the RAA contains certain obligations for registrars with regard to the collection and publication of WHOIS data on all gTLD domain name registrations. Specifically, this includes the obligation to provide responses to queries within the WHOIS database. These responses frequently include the following data from registrants: domain name, registry registrant ID, registrant name, registrant organization, registrant address, registrant telephone and fax number as well as registrant email address.

4 In order to comply with current data protection laws, registrars frequently rely on consent given by registrants to include registrants' data into the WHOIS services (ICANN's contracts with registrars require them to obtain such consents). When registering a domain name, there may be the possibility for a registrant to make use of privacy or proxy services regarding the public display of WHOIS data, depending on the technical setup of the registrar. Between 20 to 25% of gTLD registrations make use of such privacy or proxy services. In this case, some or all of the listed data elements are withheld from public disclosure. However, in the case of abuse, some or all of this data may be revealed under certain circumstances.

III. Questions by IPC and answers

1. Can, under the GDPR, registrars and registries continue to rely upon obtaining consent from registrants to the uses of their data required by the WHOIS system? If so, would existing practices of registrars in obtaining and documenting consent need to change, and if yes, how?

5 Under the GDPR, registrars and registries could continue to rely upon obtaining consent from registrants with regard to the use of their data as required by the WHOIS system so long as the requirements for obtaining valid consent are met, namely Art. 4 no. 11, Art. 7 GDPR. In the following, these requirements will be outlined. Additionally, current examples of consent collection will be examined, whereas focus shall be put on those examples provided within Annex 2 of Instructions to Counsel **(extracts from publicly available terms and conditions of two leading domain registrars, one US and one European)**. Furthermore, with regard to the GDPR, potentially necessary changes will be presented. In any case, the following assessment shall solely include cases in which personal data according to Art. 4 no. (1) GDPR is processed. Registrants may also be legal persons, for whom the GDPR does not apply to the extent that no information on individuals is processed.

a) Scope of consent under GDPR

6 According to Art. 4 no. (11) GDPR, "*'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". Thus, especially the requirements of freely given, specific and informed consent (which, to satisfy those criteria, will also be unambiguous) need to be fulfilled. Art. 7 GDPR further specifies the requirements, in particular with regard to formality and withdrawal.

aa) Informed and specific consent

7 The data subject has to be sufficiently informed about the processing and the information has to be specific in order for the consent to be valid. This means that the consent request shall be declared clearly and concisely (Rec. 32 GDPR) and the extent to which consent is given needs to be sufficiently described (Rec. 42 GDPR). Only by having knowledge of all relevant circumstances will the data subject be able to assess the risks and advantages of providing consent.[1] This means that the data subject shall be informed of the purposes of the processing for which the personal data are intended (Rec. 42 GDPR). Adequate information also needs to point out specif-

[1] Ingold in: Sydow, Euroäische Datenschutzgrundverdnung, Art. 7, rec. 34.

ic third party transfers, cross-border transfers as well as the possibility to withdraw consent (Art. 7 para. 3 sent. 3 GDPR).[2]

Potential changes in comparison to example consent requests provided to counsel:

- Distinct description of the purpose of collection and processing of data
- Specific mentioning of possibility to withdraw
- Adequate and comprehensive description of processing activities themselves as well as description of third party transfers, with explicit information about the third parties and explicit description of necessary cross-border transfers ("and other processing", "may require", "transferred back and forth across international borders", "for example" is not sufficient to meet the requirements of the GDPR)

bb) Freely given

8 Any consent needs to be a "freely given" indication of the data subject's wishes, Art. 4 no. (11) GDPR. Whether consent is freely given can be assessed by taking into account Art. 7 para. 4 GDPR and Rec. 42 sentence 5 and Rec. 43 sentence 2 GDPR.

9 The GDPR itself, in Art. 7 para. 4 GDPR, states that, "*[w]hen 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*". With regard to this formulation, the assessment whether consent has been freely given shall take "utmost account" of whether the consent is conditional for the performance of a contract. This formulation leaves room for interpretation in such a way that there may be circumstances in which the performance of a contract is conditional on consent but consent may still be deemed "freely given".

10 On the other hand, Rec. 43 sentence 2 GDPR clearly states that "*[c]onsent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*". Hence, with regard to Art. 7 para. 4 GDPR, there is a possibility

[2] Stemmer in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, 01.08.2017, Art. 7 DS-GVO, rec. 55.

to freely declare consent even though it is conditional for the performance of a contract, whereas Rec. 43 sentence 2 GDPR generally assumes that consent cannot be freely given if it is not allowed separately or if it is conditional for the performance of a contract.

11 This constitutes an inconsistency between the provisions regulating the question whether consent has been freely given. Therefore, it is discussed controversially in legal literature whether the GDPR establishes a strict "prohibition of linkage" between the performance of a contract and consent. Data Protection Authorities would probably tend to a stricter interpretation and put an emphasis on Rec. 43 sentence 2 GDPR, therefore taking a strict prohibition of linkage as a basis. However, it is currently unclear which legal interpretation would prevail, as the legislative procedure does not provide for a straight view and judicial precedent is not yet available. To put it in a nutshell, with reasonable argumentation and diligent consideration by the controller (backed by respective documentation), it may be possible to link consent and the performance of services according to Art. 7 para. 4 GDPR, provided that "utmost account" was taken on the scope of a conditionality and keeping in the mind the remaining legal risk.

12 There is certainly an argument that such a link is present in the case at hand, thus necessitating "utmost account" to be taken if the consent is to be considered fully valid as a basis for processing. The performance of a domain registration contract between a registrar and a registrant could also be undertaken without the consent declaration of the data provision, since the mere performance of the domain registration and allocation of it could solely rely on the contract conclusion as a legal ground for data processing. The consent for using personal data for WHOIS services only has an indirect impact on the actual fulfilment of primary contract duties. In fact, it is necessary in order to meet the obligation of the registrar towards ICANN deriving from the RAA. This relationship, however, might be regarded as independent of the provision of domain registering services from a registrar to a registrant. Therefore, there is a considerable risk that a data protection authority would consider the consent to be not freely given due to a "linking of consent".

13 However, within the assessment whether consent has been "freely given", offering potential "privacy or proxy services" in connection with a domain registration and the respective WHOIS service may be a mitigating factor. This will be particularly the case if a data subject has the option to effectively choose to provide data for WHOIS services only in connection with such privacy or proxy services on the one hand, or may take the option and decision to provide the respective data comprehensively without privacy or proxy services. Depending on an individual legal review

of the privacy and proxy mechanisms and the involved conditions, such mechanisms may regularly provide for an active choice in how far the data shall be used. These services are already provided by many registrars (and especially by most major registrars) and it may be taken into consideration whether this option should be expanded. In some of these cases, the provision of privacy or proxy services is made subject to extra costs since it poses additional administrative overhead to the registrar. This again might restrict the mitigating impact. However, if the costs are only nominal and represent compensation for extra expenditures, this might potentially still suffice for considering the choice to be free.

Potential changes in comparison to example consent requests provided to counsel:

- Practical solutions to receive a freely given consent are either taking "utmost account" of whether the performance of a contract "is conditional on consent to the processing of personal data that is not necessary for the performance of that contract", which should be distinctly considered and thoroughly documented, or "waive" the dependence of the performance of a contract to the declaration of consent.
- Implementation of privacy or proxy services within the contractual consent process should be considered in this regard. The potential link between the performance of a contract and the declaration of consent may cease to exist if registrants can freely chose that their data does not appear on the WHOIS search by way of opting to use a privacy or proxy service.

14 Since the assessment of whether consent was freely given poses a considerable legal uncertainty, at least in case no privacy or proxy services are offered, it may be advisable to additionally rely on Art. 6 para. 1 sent. 1 lit. f) GDPR for legitimization as a "fallback scenario". According to this provision, processing shall be lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party and a balancing of interests turns out in favour of the controller or third party. Hence, the controller would have to examine the circumstances of a data processing procedure also in the light of Art. 6 para. 1 sent. 1 lit. (f) GDPR, taking into account the three-part structure laid out in Art. 6 para. 1 sent.1 lit. f) GDPR and comprehensive documentation methods (see elaborations for question 2 below). Privacy or proxy services would also play a positive role in the context of assessing whether a processing may be based on legitimate interests.

cc) Formal requirements

15 A declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form. It is controversially discussed whether this obliges the controller to emphasize the consent declaration. According to the wording and the common practice of data protection authorities, it may well be argued that specific form requirements should be implemented, such as highlighting, bold-print text, framing, colourful separation, or requiring a separate consent for processing.[3]

16 Moreover, a demonstration requirement emerges regarding both the obtaining as well as lawfulness of consent declaration (Rec. 42 GDPR). This is to be read in conjunction with Art. 5 para. 2 GDPR ("accountability") as well as Art. 24 para. 1 GDPR. According to these provisions, the controller shall ensure and be able to demonstrate that processing is performed in accordance with the GDPR, especially by implementing appropriate technical and organisational measures.

Potential changes in comparison to example consent requests provided to counsel:

- Emphasize the consent declaration e.g. by highlighting, bold-print text, framing, colourful separation
- Implement sound documentation procedures in order to fulfil both accountability and lawfulness demonstration obligations
- Consent declarations should be stored in an electronic format, with comprehensive verification and backup options, and meet generic protocol requirements for sound demonstration purposes

dd) Withdrawal of consent

17 Art. 7 para. 3 sent. 1 GDPR establishes the right of the data subject to withdraw the consent. This possibility persists "at any time". No restrictions as to the scope of the withdrawal have been regulated in the provision.[4] Thus, no specific requirements have to be met to exercise the withdrawal right.[5] Moreover, withdrawing consent shall be as easy as giving consent, Art. 7 para. 3 sent. 4 GDPR.

[3] Schulz in: Gola, DS-GVO, Art.7, rec. 41.
[4] Ingold in: Sydow, Europäische Datenschutzgrundverdnung, Art. 7, rec. 46.
[5] Schulz in: DS-GVO, Art. 7, rec. 54.

18 A withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. However, this does not mean that the regular data stock shall remain preserved. Rather, all data subject to the original collection based upon consent shall be deleted at the time of the withdrawal.[6] Even though it is partly discussed in German legal literature whether withdrawal may be excluded under specific circumstances (especially taking into account Art. 17 para. 1 lit. b) GDPR), the interpretation of the relevant provisions does not suggest this. Therefore, it should be assumed that the wide scope of data subjects' withdrawal rights is also applicable in the case at hand.

19 According to this rather broad scope, it would not make a difference as to the validity of exercising the withdrawal right whether registrants always have the option of registering in a ccTLD, which generally make less contact information publicly available, or whether registrants always have the option of subscribing to a privacy/proxy service under which some or all of their contact information would be withheld from disclosure to the general public. However, the activation of privacy or proxy services may potentially be a viable way of complying with a withdrawal of consent for personal data to publicly appear in the WHOIS search. It should be noted that in case consent was withdrawn, it may be discussed whether the cancellation of the registration would be a permissible consequence of exercising the withdrawal right. On the one hand, Rec. 42 sent. 4 GDPR explicitly states: "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment." On the other hand, if consent was deemed conditional but still freely given (as described above), it may be argued, also from a contractual point of view, that in such a case the cancellation could be a legally valid procedure. This would be subject to the specific circumstances as well as the contractual setup of the domain registration.

b) Summary of findings regarding consent

20 The current examples of consent requests do not match the GDPR requirements regarding valid consent declarations. There is a considerably higher transparency need, a higher need for specification with regard to distinct descriptions of kinds of data involved, recipients and international transfers, as well as higher formal requirements. Thus, the current structure needs to be changed according to the above mentioned remarks.

[6] Ingold in: Sydow, Europäische Datenschutzgrundverodnung, Art. 7, rec. 48; Stemmer in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, 01.08.2017, Art. 7, rec. 91.

21 In any case, there is a risk that any consent collected by registrants would not be deemed "freely given" by a data protection authority, and thus the consent declaration would be invalid. Moreover, consent declarations could be withdrawn without being subject to further restrictive requirements. Hence, if consent has been withdrawn, the original consent declaration would not subsist and all data within WHOIS directories would have to be deleted if their existence in these directories is based on the data subjects consent. However, to the extent privacy or proxy services are used in a reasonable scope and the registrant can freely choose whether his data appears on the WHOIS search, the consent declaration might be considered as being freely given. In any case, even if consent shall be used as basis for data processing involved with the WHOIS search, it may be advisable to rely on Art. 6 para. 1 sent. 1 lit. f) GDPR as a "fallback scenario" (see elaboration in No. 2 below).

2. Irrespective of consent, can the uses of data included in the WHOIS system by the registrar, registry and third parties intellectual property right holders using WHOIS qualify as legitimate interests for the purposes of Article 6(1)(f) GDPR? Is the analysis affected by the fact that the WHOIS database is publicly available and so could be used for purposes that may not be deemed "legitimate interests"?

22 To assess whether the use of data included in the WHOIS system by different stakeholders may be justified by Art. 6 para. 1 sent. 1 lit. f) GDPR, the controller or a third party needs to have "legitimate interests" regarding the processing. However, the existence of "legitimate interests" alone is not sufficient to allow data processing under Art. 6 para. 1 sent. 1 lit. f) GDPR. Additionally, an examination of the necessity of the processing as well as a specific balancing of interests of these interests of the controller/third party and those of the data subject in question have to take place.

a) Art. 6 para. 1 sent. 1 lit. f) GDPR as a "fallback scenario"

23 In case a statutory lawfulness exemption is used as a "fallback" to the processing on the basis of informed consent, it should be made clear to the data subject that both lawfulness exemptions may apply prior to any processing. In the case at hand, this would mean that when potentially collecting consent declarations by registrants, they should be informed that processing may also be based on the balancing of legitimate interests in favour of the controller. Otherwise, when the registrant has not been informed in such a way and makes use of its withdrawal right regarding its

consent, relying on the statutory lawfulness exemption may be deemed contradictory by a supervisory authority.[7]

b) What is the meaning of "legitimate interest" in the sense of Art. 6 para. 1 lit. (f) GDPR and which data uses does it entail?

24 Art. 6 para. 1 lit. (f) GDPR allows data processing if it "*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*". It imparts a three-part structure: data processing is allowed if (i) the controller or a third party has "legitimate interests" in the processing procedures, (ii) the processing is "necessary" and (iii) a weighing of interests turns out in favour of the interests of the controller or third party.

25 According to Art. 6 para. 1 sent. 1 lit. (f) GDPR, a controller or third party must inter alia be able to present a legitimate interest in the data processing. The term "legitimate interest" is not defined in the GDPR. Rec. 47 sentence 2 GDPR barely concretizes it in such a way that a legitimate interest "*could exist for example where there is a relevant and appropriate relationship between the data subject and the* controller". A "relationship between the data subject and the controller" is thus an example of a case in which a "legitimate interest" may exist, but is not a precondition for a legitimate interest.

26 Taking into account current interpretations of the term legitimate interests and also the structure of Art. 6 para. 1 sent. 1 lit. (f) GDPR in connection with Rec. 47, ultimately, the term "legitimate interest" should rather be understood in a broad sense, generally including all interests acknowledged within the legal order.[8] This would for example entail interests pursued for IPR enforcement, general anti-abuse protection, general consumer protection or law enforcement. Accordingly, Rec. 47 GDPR does not predetermine a strict interpretation but leaves room for a wide understanding ("legitimate interest could exist *for example*", Rec. 47 sentence 2 GDPR, specific processing "*may* be regarded" as carried out for a legitimate interest, Rec. 47 sentence 7 GDPR).

[7] Kühling in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, 01.08.2017, § 4a, Rn. 9.
[8] *Frenzel* in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Edition 2017, Art. 21, rec. 71; Plath in: Plath, BDSG/DSGVO, 2. Edition 2016, Art. 6, rec. 21.

27 Moreover, the original draft of the GDPR of the European Commission from 25 January 2012 ("GDPR[Commission]"),[9] did not entail any concretization of the meaning of "legitimate interests". Within the legislative proceedings, the version by parliamentary rapporteur Jan Philipp Albrecht from 17 December 2012 ("GDPR[Rapporteur]")[10] by contrast comprised a specific catalogue of processing situations and clarified which of these situations should be seen as entailing a "legitimate interest".[11] This catalogue was subsequently reduced within the version by the European Parliament from 12 March 2014 ("GDPR[Parliament]"),[12] including only clarifying references within the Recitals. At last, this reduction was further pursued in the negotiations between the Council of the EU and the Parliament and ultimately, only the term "expectations" by a data subject was upheld as a criterion for the interpretation of "legitimate interests". From our point of view, taking into account the rather "open" wording in the recital and this "reduction process", it can very well be argued that the European legislator did not want to regulate specific indications as to the interpretation of a "legitimate interest" and therefore set up a rather wide scope.

28 This means that basically every substantiated interest by either a controller or a third party (or both) may serve as "legitimate interest", including for example interests expressed by third parties in connection with the WHOIS procedure as set out in the "Personal Data 'Use' Matrix".[13] However, these legitimate interests also correlate with the purpose of the data processing, which has to be determined specifically and prior to any data collection by a controller. As of now regarding ICANN, it has never formally adopted a statement of the purpose of collection and processing of WHOIS data. Moreover, registrars would have to set out the specific purpose prior to any data processing. Generally, it is acknowledged that the identification of operators of intellectual property infringing sites may play a primary role here, as well as contact opportunities towards persons technically responsible for networks in case of problems. Accordingly, for example Art. 16 para. 1

[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) = COM/2012/011 final.
[10] Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) = (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))
[11] *Albrecht*, CR 2016, 88 (92).
[12] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).
[13] Available under https://www.icann.org/news/blog/personal-data-use-matrix-now-available-for-public-review, as indicated by IPC via mail from 20 September 2017.

of Regulation 874/2004/EC[14] stipulates that the "purpose of the WHOIS database shall be to provide reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names under the .eu TLD".

29 These purposes would have to be individually determined and distinctly described by a controller. This obligation derives from Art. 5 para. 1 lit. (b) GDPR, according to which personal data shall be collected especially for specified and explicit purposes. A controller may thus especially indicate measures to fight IP infringement or consumer protection as processing purposes.

30 In any case, as regards a legitimate interest by a third party, the connection between a controller and a data subject may solely play an indirect role, since the third party frequently does not maintain an immediate relationship with the data subject. In the case at hand, this would mean that the legitimate interest of a third party such as ICANN or for example another entity seeking information for IPR infringement tracking (as opposed to the registrar as controller towards the data subject) would have to be taken as a basis (Rec. 47 sent. 1 GDPR). Hence, if the relation between a controller and a data subject provides for such a third party to propound corresponding legitimate interests, these may be deemed admissible by the third party for a processing based on Art. 6 para. 1 sent. 1 lit. f) GDPR. In short: If the third party bases its legitimate interests on IPR enforcement, general anti-abuse protection, general consumer protection or law enforcement and these interests relate to the connection between the controller and the data subject, which will regularly be the case, these legitimate interests may also be seen as potentially expected by the data subject.

Impact on WHOIS procedure:

- "Legitimate interests" to be understood broadly, including all interests acknowledged within the legal order
- Also interests by third parties to be taken into account due to clear wording of the GDPR
- Legitimate interests by third parties should correlate with the purpose of the processing, which needs to be determined specifically by the respective controller
- The current handling of purpose limitation principles should be reviewed, as generally every controller would have to determine and describe the respective purposes of their

[14] COMMISSION REGULATION (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration.

data processing prior to collection and use of the data, also and specifically regarding WHOIS measures, and potentially provide information on applicable third party interests

c) Necessity and balancing of interests

31 According to Art. 6 para. 1 sent. 1 lit. f) GDPR, processing shall be lawful only if and to the extent that 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. Thus, even though legitimate interests may exist, specific focus should be put also on the necessity and the balancing of interests.

aa) Necessity

32 The data processing shall be necessary for the purposes of the legitimate interests of the controller or third parties. The necessity requirement is a requirement deriving from the "proportionality" assessment according to European law. A measure would be seen as "necessary" in case it is the mildest of a variety of equally effective measures. Only this mildest measure would be deemed to be "necessary" and thus admissible within a balancing of interests. Regarding data processing in the case at hand, it has to be determined whether the mere collection and use of WHOIS data for WHOIS services is the mildest of potentially diverse measures to provide WHOIS services to the public. In that regard, it may be necessary to consider that data processing within privacy or proxy services may be deemed a milder measure as compared to such processing without further safeguards. To ultimately determine the necessity, it should be evaluated whether including privacy or proxy services into the WHOIS service provision would still satisfy the purpose of WHOIS services to the same extent.

33 The Article 29 Working Party stated[15] that "*where an individual registers a domain name, (…) while it is clear that the identity and contact information should be known to his/her service provider, there is no legal ground justifying the mandatory publication of personal data referring to this person. (…) The original purpose of the Whois directories can however equally be served as the details of the person are known to the ISP that can, in case of problems related to the site,*

[15] Art. 29 Working Party, Opinion 2/2003 on the application of the data protection principles to the Whois directories, WP76, p. 3.

contact the individual". Therefore, it may be argued that a limited approach to WHOIS search, for example a restriction to and handling by the provider, may be deemed a milder measure as compared to the current approach by a supervisory authority. Thus, the option to implement privacy and proxy measures should be regarded as a useful tool to support the "necessity" within the assessment of the lawfulness of processing for WHOIS purposes.

Impact on WHOIS procedure:

- "Necessity" of the processing should be taken into account
- Privacy and proxy WHOIS mechanisms should be regarded as useful mitigating tools

bb) Balancing of interests

34 Ultimately, the actual balancing of interests needs to be undertaken. To carry out the balancing test the nature and source of the legitimate interests on the one hand and the impact on the data subjects on the other hand should be considered.[16] Accordingly, as also stated within Rec. 42 GDPR, the reasonable expectations of the person concerned or the foreseeability (industry standards) of the processing as well as the connection between the controller and the data subject must be taken into account.[17]

(1) Purpose of processing and correlating legitimate interests of controller or third party

35 Generally, registrars would have to determine and describe the purpose of their processing beforehand. This might entail a concrete description of own contractual purposes, and also a description of interests for which the actual data processing takes place, such as the reasonable operation of the WHOIS services. Moreover, the purposes of the legitimate interests pursued by a third party may also be taken into account, Art. 6 para. 1 sent. 1 lit. f) GDPR (see also above marginal number 30). It is thus on the one hand to be reverted to the interest and purpose followed by the controller for the collection of the data and the provision within a WHOIS measure, such as to provide contact measures in case of technical problems. The main purpose of the processing is the fulfilment of the domain contract on the one hand and the provision of WHOIS ser-

[16] Art. 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, 33.
[17] Albers in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, 01.08.2017, Art. 6, DS-GVO, rec. 53.

vices as a contractual obligation towards a third party (owards ICANN, pursuant to the RAA). Moreover, Art. 16 of Regulation 874/2004 may be deemed as another example for a legitimate purpose (see also above margin no. 28), however only in the context of setting up the .eu TLD. Data subjects have the opportunity to use privacy mechanisms, depending on the registrar.

36 On the other hand, there may be a legitimate interest to satisfy the general public with WHOIS services which have been available over many years since the introduction of the WHOIS protocol. Registrars do not only act in their own interest when processing data for WHOIS measures but also in the interest of the general public who may need to gather WHOIS data for their own legitimate purposes. This will also serve public enquiries to act for appropriate IPR enforcement, general anti-abuse protection, general consumer protection or law enforcement purposes. As regards a third party interest, IPR enforcement, general anti-abuse protection, general consumer protection or law enforcement may thus be considered in that regard. If these correlate with the original purpose of the data collection, this may be deemed legitimate interests of third parties in the current assessment.

(2) Impact on data subjects

37 Subsequently, the impact on data subjects has to be determined. Several elements play a crucial role here, e.g. the nature of the data, the way the data is processed, the reasonable expectations of the data subject as well as the connection between controller and data subject.

38 In this regard, the primary impact of publishing WHOIS data on such a generic and broad level may have a wide impact on the interests and fundamental rights and freedoms of the data subjects. Their data could be available online, worldwide and easily accessible. Reportedly, these data are often abused for unwanted marketing purposes, spam or identity theft.[18]

39 As regards the nature of the data, no special categories of personal data according to Art. 9 GDPR are involved in the processing. Still, personal data directly concerning immediate personal features of a person are often used when individuals are involved as registrants, such as the name, address, e-mail address or telephone number.

[18] Article 29 Working Party, Comments on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS data, Ref. Ares(2012)1125362.

40 Regarding the way the data are being processed, the data is available online, worldwide and easily accessible, and thus publicly disclosed and made accessible to a potentially indefinite number of persons. On the other hand, the data are not combined or analysed and thus no inferences would generally be established.

41 The reasonable expectations of the data subject are also relevant, and it is to be pointed out that because of the obligation of registrants to publish the data for WHOIS purposes, the data subject does not have a genuine choice regarding the processing of its data when registering a domain in a gTLD. Changing to a ccTLD would also not appear to be a mitigating factor in that respect, because these are effectively different domains and the policy for a gTLD is predetermined without influence by a data subject. It is to be evaluated whether the mere fact that such WHOIS services have been provided to the public ever since the inception of the domain name system leads to the assumption that data subjects have to reasonably expect that their data will be published in such a way. The reasonable expectations should be determined from the sphere of the data subject (bottom up rather than top down) based on their relationship with the controller, Rec. 47 sent. 1 GDPR. Even though keeping up such a process over a prolonged period of time may not necessarily be deemed a value in itself, an ordinary registrant facing a registrar entity would regularly recognize the long-established technical and organizational background of domain registrations and corresponding WHOIS services. Thus, the necessity to provide WHOIS services as a generalized public interest may be associated as a reasonable expectation of data subjects.

42 Registrar and registrant enter into a voluntary contractual relationship, which includes the necessity to process personal data with regard to contract fulfilment as well as WHOIS service provision (from a registrant towards ICANN), which will play a role in favour of the controller's interests. However, in many cases, the data subject is a natural person, and their standing against registrars may potentially be worthy of appropriate protection from a consumer protection point of view, which should also be taken into account.

(3) Balancing of interests

43 It is then to be determined whether the purpose of processing and correlating legitimate interests of the controller or third parties on the one hand and the impact on the data subject on the other hand and their balancing leads to a disproportionate impact of the data processing. The main

interests of fulfilling the domain contract and contractual obligation towards a third party (i.e., the registrar towards ICANN under the RAA), including the safeguarding of a functioning domain name system, may be regarded as having a significant importance for the allocation of unique names and addresses on the Internet as well as the coordination of all existing internet addresses, whereas the provision of WHOIS services is a vital factor to uphold these measures and serve technical and compliance interests. This is because the WHOIS protocol provides important information services regarding domain registration, delivering its content in a human-readable format. The Domain Name System (DNS) is a hierarchical distributed database to lookup information from unique names, i.e. to help people connect to resources like websites and email servers on the Internet. WHOIS provides information sufficient to contact a responsible party for a particular Internet resource who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name or the DNS name servers.[19] In that regard, it is also vital to point out that third party interests of IPR enforcement, general anti-abuse protection, general consumer protection or law enforcement play a crucial role in the persistence of an informative leverage point, whereas otherwise the goals behind such interests might not be achieved at all.

44 Meanwhile, no sensitive data of registrants is used. Additionally, reasonable expectations of data subjects would usually include the processing of their data for WHOIS purposes, which strongly argues for the controller's interests. Still, the rather broad availability of different kinds of data in the light of an online, worldwide, public accessibility may be deemed a further argument of the impact on the data subject. This wide ascertainment should be compensated by tackling it individually, including the introduction of additional safeguards within the processing procedure. It is also to be pointed out that actual selection options on the side of a data subject (e.g. via privacy/proxy services) would have a positive impact on the balancing in favour of the processing entity.

45 With that in mind, the actual quantity of data provided within a WHOIS request plays an important role within the balancing procedure. Since especially registrant name, organization, street, city, state/province, postal code, country, phone, fax as well as email are largely provided, this depicts a rather extensive disclosure. Thus, in the light of the varying purposes, this wide scope of available data should be re-evaluated. It has to be evaluated whether the provision of less data within

[19] See https://whois.icann.org/en/technical-overview for further information on the interplay of the DNS and WHOIS.

the WHOIS procedure would still fit the purpose of providing information to technical support or legal compliance seeking users of the WHOIS system (data minimization principle). Moreover, the implementation of technical and organizational measures as well as privacy enhancing technologies – for example, use of CAPTCHA screens, or reasonable throttling to prevent very high volume requests ("rate limitation") – may be taken into account as to whether they may serve to further prevent misuse of WHOIS functionalities (e.g. privacy by design and default).[20] Furthermore, providing an easily workable and accessible mechanism to ensure an unconditional possibility for data subjects to make use of privacy or proxy services could be taken into account as well.

cc) Interim findings for justification according to Art. 6 para. 1 sent. 1 lit. f) GDPR

46 According to the above balancing of interests based on the facts provided, there are reasonable arguments that a balancing would at least lead to a slight outweighing in favour of controller or third party legitimate interests, leading to a potential possibility to keep up processing under Art. 6 para. 1 sent. 1 lit. f) GDPR. However, to reach a more secure and reliable approach, further measures, as described above, should be implemented to safeguard that the balancing would also be seen as permissible by a data protection authority or a court. In case further security mechanisms are put in place, this would lead to a higher emphasis on the controller's or third party's interests and ultimately to a balancing in favour of the controller or a third party.[21]

Impact on WHOIS procedure:

- Consider implementing and defining clear instructions to implement privacy or proxy services and present these to registrants in an easily perceptible way
- The range of personal data elements collected and published through WHOIS could be re-evaluated in a review procedure, to achieve data minimization without unduly compromising the legitimate interests that justify processing
- Inclusion of technical and organizational measures and privacy enhancing technologies to be examined (such as captcha and other related measures, e.g. time limits, spam-shield, to be further evaluated)

[20] See also Art. 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, 42.
[21] Reimer in: Sydow, Euroäische Datenschutzgrundverodnung, Art. 6, rec. 63; Schulz in: Gola, DS-GVO, Art. 6, rec. 53.

dd) Right to object

47 In any case, it is to be observed that a data subject generally has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on Art. 6 para. 1 sent. 1 lit. f) GDPR (see Art. 21 para. 1 sent. 1 GDPR). The situation is comparable to the one described above regarding withdrawal of consent. However, there is a significant difference as to the withdrawal right: the controller may still demonstrate compelling legitimate grounds for an ongoing processing of the data irrespective of an asserted right to object. The prerequisites have to be determined in the individual case, whereas the impact may be less strict and restrictive as compared to the withdrawal right mentioned in connection with consent above.

3. Summary

48 As regards WHOIS services, changes to the current structure of fulfilling the consent exemption should be implemented. The legitimacy of consent is controversial in the case at hand, especially because of the potential “linking of consent” and the withdrawal right remaining with the data subjects. However, these obstacles may not be insuperable, and their impact might be mitigated by changing the procedures for obtaining and documenting consent, as well as by focusing on privacy and proxy mechanisms. .

49 Furthermore, Art. 6 para. 1 sent. 1 lit. f) GDPR should be taken into account as a “fallback” lawfulness exemption. Here, a considerable balancing of interests is necessary to determine whether the processing of personal data may be undertaken. Especially, the existence of “legitimate interests” alone is not sufficient to justify data processing, but rather also an examination of the necessity of the processing as well as a specific balancing of interests of the controller and a data subject will have to take place. If the collection and publication of personal data included in WHOIS were re-evaluated in a review procedure, and technical and organizational measures and privacy enhancing technologies such as CAPTCHA were examined, a balancing of interests may emerge in favour of the controller or a third party.

50 This legal assessment is based on the legal material available for the GDPR, which is currently limited, as no binding supervisory authority decisions have been taken and no case law is available. Above elucidations, taking into account the current state of affairs, provide for a sound argu-

mentation basis with regard to the processing procedures as long as the decision making processes as well as the balancing of interests are documented and the general development of the application of the GDPR is continuously followed.

sgd. Paul Voigt, Fritz-Ulli Pieper
24 October 2017