
IPC Early Input Comments on the Temporary Specification

The Intellectual Property Constituency (IPC) of the GNSO appreciates this opportunity to share our thoughts on the Temporary Specification for gTLD Registration Data. See <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>

IPC members have a strong and abiding interest in reliable, consistent access to accurate gTLD registration data. The IPC's active participation in the debates within ICANN about WHOIS and RDS over the past decade plus reflect our commitment to preserving the utility of this critically important tool on behalf of consumers, brand and IP owners, and internet users, all who rely on a safe and secure Internet. To that end, the IPC submits the following comments that highlight our areas of interest and concern.

On ICANN's Mission – Purpose(s) for Collection and Purpose(s) for Access

The IPC supports ICANN's statements to the Article 29 Working Group on May 10, 2018¹ regarding the breadth of ICANN's Mission, as laid out in the Bylaws. ICANN CEO Göran Marby's statements, in particular the references to consumer trust, consumer protection, malicious abuse, and security concerns are notable as we consider purposes for collection of data and purposes for access of data. Clearly the "resilience, security and/or stability of the DNS" extends beyond mere technical functioning. As reflected in contractual obligations and policies developed under the ICANN multistakeholder process (and discussed in brief below), combatting abuse, protection against IP infringement, and assisting law enforcement all fall within the mission of ICANN. References to ICANN's mission should not be used to limit the consideration of collection or access of data based on legitimate interests that are not technical in nature.

That being said, the IPC notes the assertion of other community members that the purposes for collection of data are limited and narrowly defined. We note that this ***does not correspondingly limit*** the necessarily more numerous and broad purposes for downstream access to data. The IPC can support limited purposes for collection, **ONLY IF** those purposes also include registrant accountability and communication with the registrant and **ONLY IF** the limited purposes for collection do not constrain later access to data solely for those purposes for which data was initially collected. If the group entertains limiting purposes for access to mirroring those purposes for initial collection, the IPC reserves the right to reopen the group's analysis on purposes for collection.

¹ See, <https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-10may18-en.pdf> (Retrieved August 30, 2018).

On the Need for a Balancing Test and Defining Legitimate Interests

Sections 4.4, Appendix A.4.1, and Appendix C.2 of the Temporary Specification describe the need for a “balancing test” when processing Registration Data in a GDPR compliant manner. The IPC notes that while Article 6(1)(f) is subject to a balancing test, other lawful grounds for processing are not, and the Temporary Specification does not appropriately reflect the GDPR in that regard.

Article 6(1)(f) of the GDPR states that processing shall be lawful if: *“processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”*. The rest of Article 6(1) provides numerous grounds for lawful processing without an exemption requiring a balancing test. (e.g.: processing necessary for the performance of a task carried out in the public interest, processing necessary for the performance of a contract to which the data subject is party).

Further, Article 6(1) states: *“Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks”*, demonstrating that the balancing test is not to apply to all purposes for processing. Article 2 of the GDPR also clearly states that several categories of processing are NOT subject to the balancing test of Article 6(1)(f). This includes processing for criminal law enforcement and by competent authorities for safeguarding against and the prevention of threats to public security, which falls outside the scope of the GDPR and instead is subject to [Directive \(EU\) 2016/680](#).

The sections of the Temporary Specification listed above do not recognize that there are categories of processing of Personal Data in Registrant Data that should not be subject to the qualification of “not overridden by the fundamental rights and freedoms of individuals whose Personal Data is included in Registration Data.” The IPC has consistently voiced its concern that the Temporary Specification does not make note of these important clarifications and limitations in the GDPR, thereby resulting in an overapplication of GDPR. This needs to be addressed.

For processing that is necessary for the purposes of the legitimate interests pursued by the controller or third party, it is clear that the balancing test of Article 6(1)(f) applies. Legitimate interests under Article 6 pursued by a controller or third party are not yet defined. We support identifying categories of legitimate interests and purposes that qualify for processing in accordance with Article 6(1)(f) of the GDPR and we recommend that the Consensus Policy should not seek to exclusively define such interests by using language such as “only for the following legitimate purposes.” Any section defining legitimate purposes should allow for changes, additions and edits.

On the Ability to Publish Registration Data with Consent

Section 7.2.1 of the Temporary Specification mandates Registrars to: *“provide the opportunity for the Registered Name Holder to provide its Consent to publish the additional contact information outlined in Section 2.3 of Appendix A for the Registered Name Holder”*. However, Section 7.2.2 gives Registrars

the option to: “provide the opportunity for the Admin/Tech and/or other contacts to provide Consent to publish additional contact information outlined in Section 2.4 of Appendix A”.

The IPC recommends that the final consensus policy of the EPDP should ensure that the opportunity to Consent to the publication of any RDDS data fields MUST be extended to both the Registered Name Holder and any Admin/Tech and/or other contacts². Therefore, we suggest that the word MAY in section 7.2.2 should be a MUST.

On the Territorial Scope of the GDPR and Redaction of RDDS Data of Legal Persons

Appendix A.3 of the Temporary Specification allows Registry and Registrar operators to apply GDPR obligations beyond what is required. Specifically, it allows the application of the GDPR to be applied to Registrants outside of the EEA and to registrants which are legal persons. The IPC recommends that the final Consensus Policy of the EPDP limit the modification of WHOIS accuracy and transparency requirements to personal data that explicitly falls within the scope of the GDPR.³

We agree that any contract modification for compliance with GDPR must be applied to all contracted parties and registrants within the EEA. However, we disagree that it should, or even could be applied globally, particularly in cases of a non-EU establishment and a non-EU data subject. This is a substantially overbroad application of the GDPR that goes well beyond the territorial scope of the GDPR and is directly contrary to ICANN’s consensus policies on WHOIS and ICANN’s stated aim of preserving the existing WHOIS system to the greatest extent possible.⁴

Second, as ICANN has acknowledged, data of “legal persons,” to the extent such data does not contain “personal data,” is not within the scope of the GDPR. The GDPR, by its own terms, expressed clearly in Article 1(1) applies only to the: “protection of natural persons with regard to the processing of personal data.” We disagree with ICANN’s position not to require a distinction between data of natural versus legal persons. Instead, the model must require such a distinction; to treat registrations of natural and legal persons the same would be overly broad and unwarranted by the GDPR and not in keeping with ICANN’s mission.⁵ Accommodating efficiency and expediency concerns of Contracted Parties is not

² See e.g. [IPC Submission to the LG Bonn Court and the Higher Regional Court in Cologne Regarding ICANN vs EPAG Case, July 16, 2018](#), in which the IPC fully explains the utility of continued collection of Administrative, Technical, and other contacts. (Retrieved August 30, 2018).

³ Intellectual Property Constituency Comments on Proposed Interim Models for ICANN Compliance with EU General Data Protection Regulation, January 29, 2018 at <https://www.icann.org/en/system/files/files/gdpr-comments-ipc-icann-proposed-compliance-models-29jan18-en.pdf>. (Retrieved August 31, 2018).

⁴ See e.g.: GDPR, Art. 3 (the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union, or data subjects in the Union); Hamilton Memo Part 1, Section 3.2.1 - 3.2.2.; Hamilton Memo Part 2, Section 2.1.4; GAC Feedback on Proposed Interim Models for Compliance, p. 7, Section IV(D); Data Protection and Privacy Update – Plans for the New Year (“We’ve made it a high priority to find a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible.”).

⁵ See e.g.: GDPR, Art. 1. (the regulation applies to the protection of natural persons with regard to the processing of personal data); GDPR, Art. 4. (personal data means any information relating to an identified or identifiable natural person); Hamilton Legal Memo Part 1, Section 3.5.1 (“[D]ata processed through the Whois services will not be covered by the GDPR if it relates solely to a legal person.”); Taylor Wessing Legal Memo, p. 4

adequate justification for an overbroad application of the GDPR. Further, while some Contracted Parties have claimed it is not feasible to draw these necessarily distinctions, we know that it is feasible for contracted parties to easily differentiate between natural and legal persons, and between registrants in the EEA and registrants elsewhere. Multiple contracted parties already do so, employing a myriad of methods. Some IPC members do the same, at scale.

On the Redaction of Email Address and City

Email address is the primary means of contacting the registrant, which is a fundamental purpose of WHOIS, and is necessary to carry out a myriad of legitimate interests. Upon applying the Article 6(1)(f) balancing test and noting that publication of email address that does not contain personally identifiable information is lawful, the IPC concludes (as detailed below, and in previous comments), that registrant email address should be publicly available, whether or not that email address contains personal information.

As recently explained in the IPC letter to Cherine Chalaby dated May 11, 2018 regarding an Interim Solution for GDPR Compliance⁶, the IPC maintains the importance of keeping registrant email address publicly available for many legitimate purposes and lawful purposes for processing. There is a legal basis under Article 6(1)(f) to keep the registrant email address publicly available for the following legitimate purposes (among others): third party IP enforcement purposes arising from or related to the domains at issue; to protect Internet end users and the general public against fraud, identity theft, and various cybersecurity threats that may arise or be implicated by the domains at issue, and to protect the registrants themselves, for example in the event their domain is compromised. In all of these instances, quick access to registrant email address to contact the registrant urgently is critical.

section 5; Wilson Sonsini Legal Memo, p. 6-7 (“[I]f self-identification creates a process by means of which less personal data is included in the registration (e.g., by including only the data of legal persons, which is not considered to be personal data), then it may lower the legal risk.”); GAC Feedback on Proposed Interim Models for Compliance, p. 5 (“Legal persons are not protected by the GDPR. Not displaying their data hinders the purposes of WHOIS without being required by the GDPR. The GDPR only applies to the personal data of natural persons.”); European Commission Letter of February 7, 2018, p. 3 (“The Commission welcomes the distinction between personal data and other data (about legal persons). The GDPR only applies to personal data of natural persons and therefore does not regulate the processing of the data of legal persons (unless such data also relates to an identified or identifiable natural person).”; European Commission Letter of January 29, 2018, p. 3 (“As the GDPR only applies to personal data of natural persons, in a first step, a distinction should be made between data that fall within the scope of the GDPR and other data elements.”); Article 29 Working Party Letter of December 6, 2017, p. 1 (referring to limitations on publication of “personal data of individual domain name holders”).

⁶ <https://www.icann.org/en/system/files/files/gdpr-comments-ipc-icann-proposed-compliance-models-11may18-en.pdf>. (Retrieved August 31, 2018).

Detailed legal analysis provided with the IPC Letter from Brussels-based law firm Petillion⁷, and legal analysis provided with a letter from IPC Member, COA (Coalition for Online Accountability)⁸ performed by Bristow's⁹, a prominent UK-based law firm with a specialized GDPR Compliance practice, concludes (in part) that the legitimate purposes enumerated above (and others) are proportional to, and not outweighed by the privacy interests of the data subject, not least because the data subject need not put personal data in the email address used for registration. This satisfies the balancing request demanded by Article 6(1)(f) on its face, resulting in the conclusion that the registrant e-mail address should be publicly available, in compliance with GDPR, and should not be redacted by default.¹⁰

The IPC has noted that anonymized email addresses and/or web forms are not an adequate solution to the IPC's concerns about obtaining registrant email address in furtherance of the legitimate purposes noted. In particular, anonymized email addresses and web forms do not enable a third party to determine whether the registrant actually received the email pursuant to "bounce-back" information. Also, web forms do not permit the IP community to send notices to the registrant commensurate with the scale of infringement that may be occurring over the registered domain(s). In addition, registrant email is a key means of correlating various domain names registered by a single registrant, even where other data is unavailable or inaccurate (e.g.: "Reverse WHOIS").¹¹ The brand and IP community have already noted hundreds of instances in which the absence of Reverse WHOIS has harmed their ability to enforce quickly and efficiently against malicious domain names. If there is a technically feasible way to maintain the ability to confirm receipt of an email and correlate various domain names registered by a single registrant (e.g.: pseudonymization), the IPC could support a pseudonymized email solution.

Finally, the IPC also maintains that Registrant City is improperly categorized as personal data and thereby improperly redacted from public WHOIS. Registrant City is critical information in determining venue for legal proceedings, including lawsuits filed against the Registrant, and contacting local law enforcement. It is unclear how these important legitimate purposes for processing such data would be balanced in favor of redaction by the registrant's rights in that data.

⁷ Petillion Letter to European Authorities re: GDPR and WHOIS: Impact on Law Enforcement, IP rights and consumer protection – Digital Economy, May 11, 2018. <https://www.icann.org/en/system/files/files/gdpr-attachment-1-ipc-icann-proposed-compliance-models-11may18-en.pdf>. (Retrieved August 31, 2018).

⁸ Comments of the Coalition for Online Accountability on Public Availability of Registrant E-mail, May 11, 2018. <https://www.icann.org/en/system/files/files/gdpr-comments-coa-icann-proposed-compliance-models-11may18-en.pdf>. (Retrieved August 31, 2018).

⁹ Bristow's LLP Memorandum on Publication of Registrant's Email Address, May 8, 2018. <https://www.icann.org/en/system/files/files/gdpr-attachment-1-coa-icann-proposed-compliance-models-11may18-en.pdf>. (Retrieved August 31, 2018).

¹⁰ We also note that EURID, the operators of .eu, which are also subject to GDPR, do publish email address as a matter of course.

¹¹ Joint IPC & BC Comment on Draft Interim Model for GDPR Compliance, February 28, 2018. <https://www.icann.org/en/system/files/files/gdpr-comments-joint-ipc-bc-icann-proposed-compliance-models-28feb18-en.pdf>. (Retrieved August 31, 2018).

On Defining Reasonable Access

Section 4.2 of the Temporary Specification describes the obligation for Registrars and Registries to provide “reasonable access to Personal Data in Registration Data to a third party...”. The IPC supports this section and strongly believes that the EPDP is responsible for developing policy that defines the term “reasonable access”, thereby enabling access to WHOIS data as permitted by GDPR. This includes implementation via the RDAP protocol.

Regarding providing reasonable access, the IPC believes that 90 days is too long. We suggest that access should be required as soon as commercial feasible but in no event longer than 15 calendar days, which is consistent with the time period in which Registrars must comply with the requirements of the current WHOIS Accuracy Specification under the 2013 RAA, unless the time period for publication or disclosure is otherwise specified by the applicable legislation, court order, or other binding legal authority.

On the Continued Use of the WHOIS Conflicts Procedure

Appendix C.1 of the Temporary Specification lists several principles to govern the processing of personal data in the WHOIS system, “except as required by applicable laws or regulations.”

We note that all obligations are subject to applicable laws, therefore, for the sake of certainty, it is important that the obligations be clear and certain, and not subject to any one party’s view of what applicable laws require. There is an existing policy and process to govern conflicts between WHOIS obligations and National Data Protection Laws¹², that must govern any conflict between those laws and such obligations. The language above appears to allow circumvention of that policy and process and creates uncertainty.

Because of this uncertainty, the IPC recommends that equivalent language in the EPDP final Consensus Policy should be modified to ensure certainty. For example, the phrase “except as required by applicable laws and regulations” should be deleted, as it is unnecessary and creates confusion as to the applicability of the WHOIS Conflicts procedure.

On Important Implementation Issues Raised in the Temp Spec Annex.

As discussed extensively by the GNSO Council during the drafting of the EPDP Charter, the IPC maintains that the reference in the Annex to continued community work on developing an accreditation and access model demonstrates that this issue is clearly deemed to be essential to the future of the

¹² Revised ICANN Procedures for Handling WHOIS Conflicts with Privacy Laws. Effective date April 18, 2017. <https://www.icann.org/resources/pages/whois-privacy-conflicts-procedure-2008-01-17-en>. (Retrieved August 31, 2018).

ICANN policy structure and system. We understand that the issue is subject to the gating questions defined in the Charter, nonetheless, submit that discussion of this issue should not be deemed separate and apart from this EPDP.

Moreover, in addition to the issue identified in point #1 of the Annex (related to an accreditation model), IPC supports continued discussion of all important issues enumerated in the Annex by the EPDP team.

Respectfully Submitted,

Intellectual Property Constituency