**Comments on GDPR Interim Compliance Models for WHOIS**

**& Associated Privacy Compliance Issues**

TheNoncommercial Users Constituency would like to take this opportunity to thank ICANN for its transparency in how it is handling GDPR compliance, and for giving us this opportunity to comment on the three proposed models. We take the liberty of commenting later on a rather fuller basket of data protection issues, because we understand that these are interim measures. We do not wish to lose this opportunity to suggest more complete responses to the problem of overcoming gaps in data protection at ICANN. Furthermore, we hope that by adding to this document to make it more comprehensive in scope, we can help avoid the confusion that newcomers to our own stakeholder group face as they try to understand this rather complex state of affairs in which ICANN finds itself.

**Executive Summary**

The short answer to the Goldilocks challenge with which ICANN has presented us, is that of the three models, none are perfect. We prefer Model 2b. It is still not quite right however, and we would like to express our endorsement of the ECO model, which is better. We would also like to note our appreciation of their workbook, which we find to be a very useful document, and a thorough and accurate legal analysis. We have explained our reasons for this choice, and the rationale for rejection of each of the other two ICANN proposed models in section I.

In section II, we have reviewed in detail the models received as of January 22, 2018. We have also reviewed the comments received to date.

In section III, which will be added in a separate submission, we provide our comments on the questions posed to Hamilton, and the legal advice received, including that which has been offered from stakeholders. In this section you will find some proposed questions that have not yet been posed to legal counsel, to the best of our knowledge. We understand that further analysis will continue after the interim measures have been adopted.

In that light, we will provide in section IV an exploration of some of the issues which we feel the focus on GDPR compliance, in the particular context of data disclosure and retention, has left relatively unaddressed, or which we wish to emphasize. Examples of these issues include:

* ICANN is the principal data controller here. Because the community has no input to the registrar accreditation agreements (RAA) and are not a party to the contract, the responsibility for WHOIS policy rests clearly on the shoulders of ICANN and not the community. The prevailing rhetoric surrounding “the picket fence” that keeps the community out of these negotiations and supports claims that the contract is not a policy instrument is unsupportable. Absent an RDS policy, and we see no signs of one emerging soon, the contract is the policy instrument, and it appears that the US government set the policy.
* The determination of who gets access to personal information is a key policy issue, and failure to figure out how to accredit those who get access has held up the development of tiered access. We do not believe that self-accreditation is an acceptable option under any circumstances, and demand a more rigorous, standards based process where independent audit is possible. We draw to your attention the fact that the right to have data protection overseen by an independent data protection authority is a right in Europe, guaranteed by section 8(3) of the European Charter of Fundamental Rights. Accepting self accreditation from those who want access to the data is putting the foxes in charge of safety in the chicken house. We include proposals for interim measures in section I of this document.
* We would remind everyone that there are now 120 data protection laws in place around the world. While few of them have fines of 4%, it would be cynical of ICANN to only move on compliance where there are aggressive enforcement measures in place. Furthermore, such an action exposes contracted parties to continued risk. The current WHOIS conflicts with law policy (or more accurately, procedure) is a failure across many factors, we simply need a privacy policy that harmonizes to the highest level now. This is the only sensible, cost effective way to deal with varying data protection laws in a global environment. Countries that insist on non-compliance with data protection best practice should be accommodated exceptionally, and be required to request access to personal data in compliance with fundamental human rights. In other words, the WHOIS Conflicts with law policy needs to be stood on its head, and become the RDS Conflicts with privacy policy instrument or procedure.

We hope that our comments are useful and will be taken as seriously as other comments in the community are. End users deserve to have their rights upheld and their perspectives represented at ICANN.

**Section I Comments on the ICANN Models**

The three models clearly follow the Goldilocks principle; Model one is too much like the status quo and clearly does not accord with the Hamilton advice received, Model 2 is better (although still not fully compliant with the GDPR), and Model 3 is interesting from a data protection perspective but very difficult to put into place. Our approach in evaluating what to do at present, given the predicament that ICANN and its fellow data controllers find themselves to be in, is based on the principles one follows in performing a risk assessment. We also base our comments on the advice that we have given ICANN over the past 18 years, the visits we have arranged from data commissioners, and the lengthy correspondence and opinions that the data commissioners have provided to assist ICANN in meeting its obligations.

Here then are some of the key risks we see in this project:

1. Lack of preparedness to meet data protection requirements
	1. There are 100 days left to reach compliance, at the time of writing.
	2. Registrars have complex systems to reconfigure. Last summer they said they needed models by September.
	3. The focus of ICANN has always been on the publication instrument and the needs of third party users…..not the registrants, and not the responsibilities of the co-controllers of the personal data.
	4. There are other instruments that handle data which have not received much focus at ICANN (e.g. zone files, the escrow data and the contracts that govern the agents etc.). These instruments or data collections also have to meet GDPR on May 25. Simply toggling the length of time that registrars are required to retain data after their needs have been served (as we see in the models) does not really address the data protection requirements beyond the WHOIS interface. We agree with the analysis in the ECO documents, but do not agree that these issues can be neglected for very long.
	5. Unfortunately, there is a long and rather fractious history of ICANN not responding to requests for compliance from the DPAs.
	6. The only mechanisms that ICANN can point to as demonstrating compliance with law at the moment are the WHOIS Conflicts with Law Policy, (which is in reality a flawed procedure not a policy), and the Registrar Accreditation Agreements, which require a forced consent for collection, mandatory enabling of bulk access for value added service providers, and mandatory publication of personal data. This does not demonstrate best efforts in our view.
	7. ICANN now has a data protection officer, but it is not clear to us that there has been staff training in privacy, expansion in the Compliance Branch to include compliance activities required in matters of data protection, data access procedures and complaints mechanisms, etc.
2. Cost allocations

 We recognize that some of the key original stimuli prompting the establishment of ICANN was a desire to open up the market, facilitate sharing of the business of domain name registration, enable competition etc. It is obvious that many of the tradeoffs made over registration data were motivated by dominant players not wishing to pay for access to the data (thus an open WHOIS), registrars not wishing to pay to protect the data from disclosure (thus paid proxy services), bulk data access required to be provided at market rates (thus data sold at reasonable rates, despite data protection law that might apply). Disruption of this information ecosystem is prompted by very real prospects of fines for data controllers, including value added service providers who have gained bulk access to date, so once again money is the driver, not policy considerations related to rights and responsibilities. There is no budget for data protection compliance in the current ICANN budget documents, and it is not clear at all who will pay for changes, notably tiered access models. In this category then we have questions about how change is going to take place over the following cost issues:

1. Closing the open system will mean higher costs for contracted parties, as they will have to deal with requests for data arriving in small numbers (not blanket access).
2. Can registrars continue to charge for proxy services when the GDPR gives rights to privacy?
3. Information aggregators have been getting bulk data at minimal or no cost, if they qualify for continued access to this data will they be able to access the data for free, and will they be able to resell the data at current rates to all current customers? The EDPS has noted that this group will be subject to the GDPR as data controllers as well.
4. Various mandatory provisions for user rights will have cost implications: consent mechanisms including providing sufficient information to make the consent an informed consent, withdrawal of consent, right to be forgotten (throughout ecosystem), access to information, rectification rights, etc.
5. Current escrow provider and transborder data flow issues, to the best of our understanding, have not yet been satisfactorily resolved between registrars and ICANN.
6. Tiered access models, which we support, have cost implications for accreditation and authentication, not to mention building the systems and automating second tier access to the extent possible. The question of who is going to absorb each of the new costs has not, to the best of our knowledge, been answered.
7. Given the possibility of Court challenges, there needs to be a contingency budget for ICANN’s costs, including the possibility that if contracted parties cannot reach compliance and are fined, they sue ICANN as Controller.
8. Communications risks

Given that ICANN has survived with a noncompliant approach to data protection for so many years, it seems unlikely that community members will take this risk seriously. Nevertheless, there are communications risks, particularly given the state of unreadiness.

* 1. A finding of non-compliance, particularly if accompanied by severe criticism and fines, may be described as a failure in accountability on the part of ICANN. This needs to be effectively countered. Good luck.
	2. Data breaches need to be informed to the relevant data protection authority in 72 hours. Failure to do so could have serious implications.
	3. Failure to reach agreement among community members about measures, both interim and long term, may escalate and have serious implications for the viability of the multi-stakeholder model.

Legal and policy risks we will describe below in the detailed commentary on the models. As mentioned previously, we endorse the analysis in the ECO documents as being the most thorough which have been presented to date.

**Approach**

In the section on approach, item 2, it is stated that the goal is to maintain the existing WHOIS to the greatest extent possible. We think the WHOIS has been broken for some years, and do not wish to maintain it.

In item 3, while we recognize that ICANN’s Bylaws have continued to consider compliance with privacy laws an exception to the policy of full disclosure, we now have data protection laws in most developed countries. It is time to harmonize in favour of compliance, not regard it as an exception. Item 4 says ICANN acknowledges that contracted parties must comply with all applicable laws. What about ICANN? ICANN is a data controller, does it not also have to comply with all applicable laws? How dare it set policy in such a way as to obstruct its contracted parties in their efforts to comply with law? How can it continue to obstruct end user rights? Bear in mind also that ICANN is a party to the escrow contracts, it has access to data therein, and all aspects of the escrow obligations must be in compliance with the GDPR (and other laws) including transborder dataflow. This is not the registrars responsibility, it is ICANN’s issue. In this respect the registrars are in our view acting as data processors for ICANN’s purposes.

In item 5, we note again that the approach to data protection compliance, and the pursuit of an overarching purpose of data processing, starts with a collection of use cases (user stories). ICANN creates policy and contractual compliance models for managing the DNS, it should start there to find its purpose for data collection, not with a canvassing of third parties as to who wants the data and for what myriad of purposes. This is absolutely backwards. Data minimization is the key, not data exploitation, no matter how worthy the cause.

**Commonalities across all models**

Data elements

The current RDS PDP may decide that there is too much data collected. It seems unnecessary to try to determine data elements that cannot be justified at this point, given the urgency, but we note that current Thick data sets may be excessive.

Performance of a contract

We appreciate that performance of a contract is a legitimate reason to collect, use and disclose data. However that contract is supposed to be guided by a defensible policy, which ICANN lacks. Current contracts cannot be assumed to be at all compliant and will have to be revised. This provision also, as the Article 29 Working Party recently pointed out, relates to contracts where the data subject is a party. It would not help with the privacy infringing provisions of the current RAA.

Consent

Section 5 seems to be quite wrong. We do not agree that registrars **must** request that users consent to the full disclosure of thick WHOIS data. First of all, we are trying to avoid the deletion of data elements because of time constraints, but we are confident that full disclosure of thick data does not comply with the GDPR. Secondly, consent is a very precarious basis for processing for a number of reasons (which are enumerated in the ECO document, we will not repeat them all here). It is almost impossible to ensure that the consent is informed, in such a complex global environment. Secondly, management of consent options (collect this, don’t collect that, display this, don’t display that, withdrawal of consent, etc.) is expensive, time consuming, and complex given the variety in relevant law. Assume a scenario where a registrar in a non-EU state, but which has a very different data protection law, is seeking consent from an EU customer. Both laws apply. This is very messy and is potentially expensive, which is why companies always try to harmonize their global policies in ways that ensure they achieve a high level of compliance. In this instance, that means GDPR.

Transfers

Care must be taken to ensure that the rights (and the data) of the registrant are protected throughout the transfer process. This is particularly true for privacy/proxy customers.

File Access and Notifications

Section 7 should note that the rather vestigial rights of correction of data (more like obligations with respect to accuracy) include rights of access and deletion.

Purpose

There has been an interminable discussion on purpose at ICANN, particularly in the current RDS PDP. We propose that you use the purpose that was agreed by the GNSO, by a supermajority vote, in 2006. It is basic and within ICANN’s remit:

The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name 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 within a [Domain Name System] name server.

The current RDS PDP has wrangled endlessly on the purpose of the registration data service, often conflating the purpose of the overall processing of data with the uses of the public disclosure instrument, the current WHOIS. It is evident that progress towards a common understanding of what exactly the data protection community understands by the term is glacially slow, and demonstrates a failure in the multi-stakeholder process. “Purpose of processing” certainly does not mean that every possible use of every possible disclosure to third parties serves to justify the collection, use and disclosure of information that is superfluous to what is required to register a domain name and put it into secure and stable operation.

We understand that the law enforcement community has demanded easy access to personal data for many years, but this flies in the face of data protection law. The fact that WHOIS has been open, and has facilitated bulk access to this data for other purposes including tools used by law enforcement and private sector security practitioners does not mean the situation has to continue thus. While it is reasonable to take some measures in processing to support combatting fraud, guarding against security risks including phishing and, pharming, and malware distribution, the purpose of the RDS cannot be retuned to read, “for the purposes of investigation of crime and Internet abuse”. ICANN is not a law enforcement agency.

Subject to this caveat, we agree that the five explanatory points listed on page 6 would indeed be desirable. Considerable refinement and definitions are required to enable this.

**The Models**

We understand that the models are not presented as 3 options to be taken intact, but rather as models with various details that could be mixed and matched. We will therefore comment on aspects of each one.

**Model 1**

Model one has various territorial or jurisdictional considerations. We would suggest that harmonizing and have all registration data follow the same policy is the cheapest and easiest way to implement the GDPR. Forget trying to decide where someone resides, or whether the data is transiting Europe for processing. Simply protect it.

The minimum dataset in Model 1 is not minimal enough. We believe, and we would cite numerous communications from the data commissioners, including the Article 29 Working Party 2003 Opinion, that name and postal address are personal information, and it is not necessary to release either element. To access data not published, we agree that third parties must be accredited and authorized. Requests must be limited and specific, and recorded. We do not believe that self certification is acceptable, and believe that professional standards must be developed under some kind of quality standards system. Such a standard would both define a professional code of conduct to for the categories of the accredited requestors, but it would also set standards for the treatment and protection of personal information that has been released to them. One-off requests, e.g. a consumer complaining about a harassing email or website, would be processed in a separate stream, as they would be assessed in a more labour intensive way. Clearly the goal in an accreditation and authorization scheme is to automate access for routine, regular requestors.

**Model 2**

Model 2 is an improvememt on Model 1, but the jurisdictional comments remain….treat all registrants the same. . We agree that not differentiating between whether a registrant is an individual or a legal person is important. Legal persons are completely at liberty to release and publish their information, and if they wish to have additional fields that serve their security needs, that should be examined in the RDS PDP. However, the rules for registration data processing must not be set according to the wishes/needs of large corporations.

We support Model 2b, although the ECO model is preferable. We repeat the caution on the use of consent for optional release of personal information: the costs of managing the consent of individuals is high, and it is impossible to ensure that individuals are truly aware of how far their data is going to travel, or how it will be combined and sold. As indicated in Model 1, we support a full standards development process to develop professional standards for parties who wish routine access to tiered data.

In terms of input on how to move forward on an accreditation scheme for tiered access, we offer the following ideas. A standards development process would require the gathering of volunteers who are willing to support it, and the collection of instruments which are currently in use in a voluntary way, among the various users of personal data (e.g. APPWG, legal practitioners). We would propose a workshop on this topic at the Annual general meeting in Barcelona, to discuss how this could be achieved. In the meantime, a draft policy for those receiving data could be developed, including the requirement that they make an undertaking that they would abide by agreed privacy standards (e.g. CAN/CSA-Q830, ISO , and other which the SSAC might help in suggesting. These parties would make specific undertakings to not release the information further unless the recipient is a signatory to the same undertakings.

**Model 3**

Model 3 does not accommodate the needs of cybercrime and trademark abuse investigators sufficiently. It is the view of many in our community that this would put too heavy a burden on registrars and registries, thus driving up the costs of domain names in an unacceptable manner. We note however that one of our members, the EFF has submitted separate comments supporting this model, and their reasons for doing so we support.

The data retention for only 60 days is the best option for a data retention regime. Given that data is in escrow and thus available in an emergency, we do not support data retention beyond what is necessary for the registrar. 60-90 days seems reasonable.

**Section II Comments on the Submitted Models**

Strawman Proposal, Greg Aaron, IThreat Cyber Group

This proposal has many good aspects to recommend it. It asks the question, “Tell me how this proposal stands up to scrutiny? Is anything unworkable?, etc. Briefly:

* Consent issues cannot be left for later analysis, they are too central to the issues at hand
* Registrars and registries cannot continue to publish what they do now
* One cannot assume that companies have obtained the consent of employees to include their names in a public directory, one has to take steps to ensure they have.
* It is risky to assume that ccTLDs are compliant with the GDPR (e.g. Nominet).
* As discussed above, differentiating between citizens of Europe, data that is passing through the EEC, etc. is just too complex for a workable system. The default has to be protection; corporations and organizations can opt out to publish data as they see fit.
* Under other necessary arrangements: Common language for data processing indeed could be developed…..this would best be done in the privacy policy that NCSG has long recommended be developed.
* The question regarding “personally identifiable data” is, with respect irrelevant for our purposes. There has been lengthy wrangling in the RDS PDP, due in the view of some of our active participants in that group to the tendancy of US members to cling to this construction of personal information, rather than the broader definition of personal information used in EU (and many other) data protection laws. See the discussion of personal information in the ECO documents, they do a good job on this analysis. We agree that it is necessary to publish the IP address, but disagree that in the current environment, only the ISP can link it to the natural person. This is an interesting question for future research.
* While the last line “The GNSO’s RDS WG closely examined the issue in 2017 and generally did not feel that any thin data fields constitute personally identifiable data” is generally accurate, representatives of NCSG disagreed strenuously with both the use of the term “personally identifiable”, as it is a red herring, and with the assertion that thin data is not personal information. Because it relates to the file of a natural person, the data is personal information. This does not of course mean it cannot be disclosed.

**Coalition for Online Accountability**

(this one is a write off, editing to be polite but thorough)

**Section III Comments on the Legal Opinions and Questions (to be submitted separately)**

**Section IV Comments on other RDS related issues**