Draft Interim Model for GDPR Compliance - IPC & BC Comments

Category	ICANN Interim Model Element	Comments	Supporting References
Must Model be applied globally or only to European Economic Area?	Must be applied to EEA, may be applied globally, but need to negotiate a Controller Agreement	We agree that any compliance model must be applied to all contracted parties and registrants within the EEA. However, we disagree that it should also be applied globally, particularly in cases of a non-EU establishment and a non-EU data subject. Details regarding ICANN's proposed "controller agreement" are too scant to allow us to support the proposed element in its current form. Contracted party expediency is not an adequate justification for a substantially overbroad application of the model that goes well beyond the territorial scope of the GDPR, and is directly contrary to ICANN's stated aim of preserving the existing WHOIS as much as possible.	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.").

Registrant Types Affected	Registrations of natural and legal persons	Data of "legal persons," to the extent such data does not reflect "personal data," is not within the scope of the GDPR. Accordingly, we disagree with ICANN's proposal not to require a distinction between data of natural versus legal persons. Instead, the interim compliance model must require such a distinction; to treat registrations of natural and legal persons the same would be overly broad, surpassing even the European Commission's own interpretation of the GDPR. Such a distinction could be implemented, for example, by registrant self-certification as to whether they are a natural person or registering the domain name on behalf of a legal person. These terms, and the consequences of the selection, would be explained up-front as part of the registration process flow. If the registrant self-identifies as a natural person, then the interim compliance model would apply. If the registrant self-identifies as representing a legal person, all registration data would be public, except: no entry for registrant name would be required (only registrant organization) and registrant name field would default to "Domain Administrator" or similar non-personal title.	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 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

		However, the individual registrant on behalf of the legal person could affirmatively opt-in to including a registrant name , if preferred. Again, this is one suggested means of accomplishing an appropriate natural vs. legal person distinction, but there may be other ways to accomplish this same goal. For example, completion of the field for "registrant organization" could be adopted as a suitable proxy for whether the registrant is a legal person, as we understand has been approved by at least one European Data Protection Authority. Ultimately, the distinction must be part of the interim model, and implementation complexities should not, in and of themselves, be sufficient justification for over-compliance and departing from the goal of preserving access to WHOIS to the greatest extent possible under the GDPR.	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").

Registrant Email in Public WHOIS?	No. Create anonymized email or a web form to contact registrant.	We prefer implementation of a purpose statement that accounts for public/legitimate interests and would make lawful the publication of certain registrant data, including the registrant's email address. The Commission's recent interpretation of the GDPR on this point aligns with our position. It reinforces that necessary for performance of a contract, necessary for the public interest, and necessary for legitimate interests are all lawful bases upon which WHOIS data can be publicly available. We strongly urge ICANN to publish registrant email, even though it could include personal data. This is the primary means of contacting the registrant, which is a fundamental purpose of WHOIS. It is also necessary to carry out myriad legitimate interests, including remedying threats to cybersecurity, vindicating intellectual property rights, and protecting consumers, and the detrimental impacts on the privacy of domain name registrants is clearly proportionate to the goal of fulfilling these legitimate interests. . An anonymized email address or web form would not adequately fulfill this purpose,	GDPR Art. 5(1)(b) (purposes for the processing of personal data must be specified and explicit). GDPR, Art. 6. (the lawfulness of processing principles in Art. 6, including: Art. 6(1)(a) (data subject has given consent), Art. (6)(1)(e) (performance of a task carried out in the public interest), and Art. 6((1)f) (processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party) provide flexibility in publishing data and providing access).

		because it is unlikely to be implemented uniformly and comprehensively by all accredited registrars, and because it would not enable a third party to determine whether the registrant actually received the email pursuant to "bounceback" information. 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"). However, if there is a technical means of accomplishing contactability with data accuracy feedback as well the correlation capability, while also providing pseudonymization for the registrant email address, we would be open to considering such measures instead of general publication of actual registrant email. However, this would be challenging to timely implement uniformly across all registrars, and the most feasible solution remains to make the registrant's e-mail address available publicly. At a minimum, registrars should be required to seek registrant consent to publish this data element for legitimate purposes.	

Self-certification Access to Non-public WHOIS? **– –** **Accreditation Program for Access to Non-public WHOIS?**	No. Create anonymized email address or a web form to contact registrant or due process. Depending on timeline, self-certification may be interim solution – – Yes, in consultation with the GAC. Individual countries to provide GAC a list of authorized law enforcement authorities to have access. GAC to develop code of conduct for non-law enforcement agencies to abide by for access to non-public WHOIS data	We understand that European Data Protection Authorities (DPAs) have indicated that a self-certification process for accessing non-public WHOIS data would not be acceptable. However, we appreciate the indication from ICANN that self-certification may be an interim solution in light of the time constraints. We strongly support self-certification as a mechanism for access to non-public WHOIS data for legitimate purposes. That said, recognizing there may be challenges with self-certification, we would be open to some form of self-certification plus credentialing as an interim mechanism for access to non-public data. This concept was discussed during a meeting between contracted party representatives and IP and business stakeholder representatives that took place on Wednesday February 21, 2018. We expect to provide specific suggestions for possible credentialing bodies that could be used, in addition to self-certification, to facilitate IP owner and business user access to non-public WHOIS data. Ultimately, we agree that ICANN will need to eventually develop and implement a true accreditation program	GDPR, Art. 6(1)(f) (processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party). Wilson Sonsini Legal Memo, p. 12 ("access to the database would be limited, such as by ICANN approving accounts before [users] were able to access it."). GAC Feedback on Proposed Interim Models for Compliance, p. 2 ("Carefully consider the details of layered access including practical details and mechanics so that the community can carefully assess the roles, responsibilities, and consequences for all parties involved and the fitness for use of possible interim models."). European Commission Letter of February 7, 2018, p. 4-5 (opining on various mechanisms for access to non-public WHOIS data). European Commission Letter of January 29, 2018, p. 4 ("[C]areful consideration needs to be given to the extent to which access to specific categories of data may continue to be public and unrestricted, or whether some restriction should be

		for access to non-public WHOIS data. Such a program will need to facilitate quick and adequate access for purposes of law enforcement, cybersecurity, and consumer protection including intellectual property enforcement. However, this kind of program will not likely be implementable prior to May 25, 2018. Accordingly, the types of certification discussed above should be considered as a stop-gap measure until a full accreditation program can be designed and implemented. Some additional specific suggestions for an interim self-certification process were discussed in prior input to ICANN, including from the IPC and COA, among others.	introduced to ensure that the accessible information is relevant and limited to what is necessary in relation to the different purposes of processing. Where specific measures to ensure the protection of personal data, of which gated access is but one option, are considered necessary, the practical needs for law enforcement authorities investigations should be duly taken into consideration."). Article 29 Working Party Letter of December 6, 2017, p. 1 ("[E]nforcement authorities entitled by law should have access to personal data in the WHOIS directories, … [and] the original purposes of the WHOIS directories can be achieved via layered access.").

In addition to these issues related to selected elements in the ICANN proposed interim model, there are elements we believe must be addressed in the model, which are currently not addressed. These are detailed below.

Category	**Proposed Interim Model Element**	**Comments**	**Supporting References**
Data accuracy	Must perform operational verification of registrant email address at time of registration. Must perform syntactic validation of registrant name, organization, physical address, and telephone number at time of registration. May perform additional verification of registrant	The GDPR includes specific requirements concerning data accuracy. The ICANN proposed interim compliance model does not currently contain any element requiring any mechanisms for ensuring that domain name registration data is	GDPR, Art. 5(1)(d) (data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed,

	data at registrar/registry option. Must re-verify or validate any data elements if provided reasonable information by third party suggesting data is inaccurate.	accurate. Publication of WHOIS data facilitates data accuracy by enabling third parties (parties other than the registrar and registrant) to identify inaccurate data and alert the registrar and/or ICANN, which in turn enables corrective measures to be taken. We note that the WHOIS Accuracy Specification of the 2013 RAA addresses this issue with validation and verification requirements, including upon notice to the registrar from a third party. The more data that is non-public, the harder it is to ensure data accuracy, as a greater burden falls to registrars to validate and verify data. We suggest that ICANN perform a further analysis and specifically address how this principle is incorporated into any interim compliance model, including consideration of our proposed model element.	are erased or rectified without delay). GAC Feedback on Proposed Interim Models for Compliance, p. 9 ("The EU Council has also recognized the importance of 'ensuring swiftly accessible *and accurate* WHOIS databases of IP-addresses and domain names so that law enforcement capabilities and public interests are safeguarded.'") (emphasis added). Taylor Wessing Legal Memo, p. 13 section 28 (citing the .EU ccTLD regulation, which states 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") (emphasis added). European Commission Letter of February 7, 2018, p. 6 (discussing accuracy of data).
Bulk / aggregated data access	Create accreditation standard to ensure consistency across providers. Accreditation must include high-speed access to bulk/aggregated data.	ICANN did not include any specific requirements in its proposed interim compliance model with respect to bulk or aggregated data access. We understand that in ICANN's view, bulk access would work no differently than general access,	European Commission Letter of February 7, 2018, p. 4 ("The access modalities should be designed to ensure that law enforcement can obtain such data *within an appropriate time frame* for the investigation, through a *single portal* for

		insofar as it simply entails a high rate of repeated and automated queries to the database, rather than individual human-directed queries. We support this interpretation, and accordingly strongly suggest ICANN explicitly include in its interim model an element that would preserve bulk/aggregated data access (e.g. through port 43 or similar automated mechanism). We suggest that unaccredited or uncredentialed parties could continue bulk access to public WHOIS data, and accredited or credentialed parties could continue bulk access to all WHOIS data.	data queries. The records should also be *searchable* in such a way as to allow for cross-referencing of information, e.g. where the same data set was used to register several sites.") (emphasis added). European Commission Letter of January 29, 2018, p. 1 ("The EU Member States have also stressed the importance of 'ensuring *swiftly accessible* and accurate WHOIS databases of IP-addresses and domain names, so that law enforcement capabilities and public interests are safeguarded.'") (emphasis added). Id. at p. 4 ("clear and workable access procedures should be put in place that meet the needs of law enforcement authorities in particular with respect to *high volumes of requests and swiftness of access*") (emphasis added). GAC Feedback on Proposed Interim Models for Compliance, p. 9 ("The EU Council has also recognized the importance of 'ensuring *swiftly accessible* and accurate WHOIS databases of IP-addresses and domain names so that law enforcement capabilities and public interests are safeguarded.'") (emphasis added).