Category	ICANN Interim Model Element	Comments	Supporting References	Implementation Notes
Must Model be applied globally or only to European Economic Area?	Must be applied to EEA, may be applied globally, subject to a data processing agreement between ICANN and the contracted parties.	We agree that any compliance model must be applied to all contracted parties and registrants within the EEA, but we disagree that it should also be applied globally, particularly in cases of a non-EU establishment and a non-EU data subject. 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 system to the greatest extent possible. It is necessary and feasible for contracted parties to draw the necessary distinction for geography. We know this because we have members who do it, at a scale.	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.").	Implementation could, for example, be automated based on registrant postal code, province or country, where false or inaccurate data provided by registrants does not create liability for contracted parties under the GDPR. This is one suggested means, but there may be other ways to accomplish this same goal.

Registrant Types Affected	The model would apply to all registrations, without requiring registrars to differentiate between registrations of legal and natural persons.	As ICANN has acknowledged, data of "legal persons," to the extent such data does not reflect "personal data," is not within the scope of the GDPR. 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. It is necessary and feasible for contracted parties to draw the necessary distinction between natural and legal persons. We know this because we have members who do it, at a scale. Ultimately, the distinction must be part of the interim model, and contracted parties' desire to avoid spending resources on GDPR implementation, as our members and companies worldwide are doing, should not, in and of itself, be sufficient justification for over-compliance and departing from the goal of preserving access to WHOIS to the greatest extent possible under the GDPR.	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.").	Such a distinction could be implemented, for example, by registrant self-certification as to whether they are a natural person (i.e. an individual) or registering the domain name on behalf of a legal person (i.e. an organization). These terms, and the consequences of the selection, would be explained in simple language 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. 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. We note that registrars must permit registrants to opt-in to full data publication, so it seems that they could implement some manner of natural vs. legal person

			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	distinction as part of the coding process for the data publication opt-in mechanism.

			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.	Publication of a registrant's email address, as verified by the registrar, along with publication of the other specific registrant data specified in the model, is needed to support public/legitimate interests. The EC's stated 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, particularly registrant email addresses, can be publicly available without violating the GDPR. In particular, publishing a registrant's email is critical because it 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. An anonymized email address or web form is unacceptable because it is unlikely to be	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).	If multiple domain names are registered using the same email address, the same pseudonymous email address must be used across all gTLDs.

		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"). We would only consider supporting a pseudonymous (not anonymous) email if it is based on validated and verified registrant information (both operationally and syntactically accurate), and is consistent across each underlying unique email address used to register any domain name across all gTLDs.		
Registry Registrant ID		In this vein, ICANN suggests the possibility of revitalizing use of the Registry Registrant ID field to accomplish the correlation function, but further details on this path are needed. This element would need to be mandatory for all registrations and be public. Since it is pseudonymous, there is GDPR support for this.		This ID needs to quickly evolve to be a global ID across all regisrars and reigstries and would need to be publicly accessible if it is to serve the appropriate cross-domain correlation function.

		In any event, other possible technical measures for achieving both contactability and correlation functions in the public data set may 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.		
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. Should the accreditation program not be ready to be implemented at the same time as the layered access model, some commentators have suggested "self-certification" as an "interim interim" solution, however this would raise a number of questions that would need to be addressed to	**Self-Certification.** We support self-certification as a stop-gap mechanism for access to non-public WHOIS data for legitimate purposes (until certification is in place for pre-approved bulk access to WHOIS information for all legitimate/public interests). **Self-Certification Plus.** We also would consider supporting some form of "self-certification plus" expedited credentialing based on existing third-party credentials as an interim mechanism for access to non-public data. **Accreditation.** We agree that ICANN needs to quickly develop and implement a true centralized accreditation/certification program 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	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.").	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. "Self-Certification Plus" means that a party desiring to "self-certify" would specify third-party credentials that it has received consistent with the stated purpose (such as membership in relevant associations). Accreditation would need to be centralized and once accredited, users must not have to be re-accredited every time they query for non-public data.

	comply with the GDPR. This will be a continued topic for discussion in the coming weeks. _ _ 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. Additional details about the proposed accreditation program for continued access to full Thick WHOIS data are	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. **Codes of Conduct.** Finally, codes of conduct should apply to all parties in the WHOIS ecosystem (including ICANN, registries, and registrars) and not just third-party WHOIS users. **Timing.** Some system for accessing non-public data must be in place as part of the interim model – this data cannot be allowed to be placed behind the gate without any mechanism for opening the gate from the start. Non-public data access must be in place or the proposed model cannot be implemented. **ICANN's access.** We note that under the proposed model, ICANN will continue to have access to all WHOIS data. ICANN must confirm that its access will be complete and automated, with no restrictions such as rate limitations. ICANN must continue to use such unrestricted access to carry out all of its obligations and operations that currently use, access, or process WHOIS data, such as contractual	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 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	

	included in Attachment 2 to the ICANN proposed model document. Additionally, Attachment 3 to the ICANN proposed model document provides a high-level diagram of a potential process for providing access to full WHOIS data.	compliance, internet security and stability, Accuracy Reporting System (ARS), and all other internal look-ups done in service of ICANN's current WHOIS related obligations and its mission to support the security, stability, and resiliency of the DNS.	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.").	
Data accuracy	The current Registrar Accreditation Agreement already includes accuracy requirements such as the validation and verification of some data elements, and the provision of notice to registrants about how to access, and if necessary rectify	We appreciate that ICANN has expressly confirmed that existing data accuracy requirements from the 2013 RAA will remain in place. However, the proposed interim model significantly hampers third parties' ability to identify inaccurate data, thus severely undercutting ICANN's accuracy requirements. Accordingly, validation of all registrant contact data at the time of registration is needed and we ask that this requirement be added. Specifically, the interim model must require registries and registrars to perform such additional operational and syntactical verification/validation at the	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, 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*	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. WHOIS accuracy must be improved in order to comply with GDPR, at the time of collection and throughout the registration period. Today's tools for registrant

	the data held about them.	time of registration and periodically throughout the life of the registration to ensure it remains accurate. GDPR does not generally apply to data that is false, inaccurate or fictitious, and such data should be thoroughly screened out. Contracted parties and ICANN, as joint controllers and processors, may face liability for inaccurate data.	*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). ICANN Bylaws, Art. 4.6(e)(i) ("Subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore	contact data verification and validation used by ICANN are unacceptable and must be enhanced, using the techniques already deployed by ICANN in other systems (such as the ARS). If registrars and registries are not required to perform additional operational and syntactical validation, then ICANN must do it independently of the contracted parties as a joint controller responsible for the quality of data.

			structural changes to *improve accuracy and access to generic top-level domain registration data*, as well as consider safeguards for protecting such data.") (emphasis added).	
Bulk / aggregated data access	Registrars would continue to follow their current practice of providing third-party bulk access to the limited set of registration data that would be available to the public. In the absence of further policy development, the *status quo* would be maintained in that additional bulk access, searchable or historical WHOIS data would not be required features.	We appreciate the explicit acknowledgement that registrars would continue to provide third-party bulk access to public data. This must require that port 43 or an equivalent protocol will remain an integral part of the WHOIS system, which is critical, without throttling limits that restrict the ability of legitimate users to access this information. ICANN's discussion regarding bulk access, searchability, and historical data calls for maintaining the status quo, but also states that these features would not be required under the proposed model. ICANN should explicitly confirm, however, that port 43 WHOIS access to third parties will continue for all public data, and also that third parties who become accredited or otherwise approved to also access non-public data would be able to then gain port 43 to access the full WHOIS data sets (public and non-public). Finally, while we understand that registries and registrars	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 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	Port 43 access should be available to approved parties for the full WHOIS data set without any throttling or other query rate limitations. This would enable bulk access to continue in a manner similar to today.

		themselves would not have any obligation to provide searchability and historical data (beyond the life plus two year retention period), third party service providers could provide these features, subject to their own GDPR compliance obligations. Finally, it is critical that once a model is implemented, ICANN will ensure that appropriate bulk access is actually being provided by all registrars and registries. If bulk access is required, but individual registrars or registries are permitted to unilaterally mask certain data or throttle the service, the entire purpose of the service would be completely vitiated. We reserve further comments on these issues pending clarification from ICANN on these points.	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).	