
Agenda Item 21: Whois Compliance With GDPR

Issue

The Whois system has made information on the individual or entity holding a domain name ("domain registration data"), available to the public. Over the past decades, this information has grown to become an indispensable tool for identifying who owns or is responsible for content, services and crime on the Internet.

As a consequence, Whois has grown to become a primary subject of attention for the ICANN Community including the GAC, in particular in relation to two particular issues:

- concerns around the lack of protection of personal data, and
- inaccuracy of registration data.

Since as far back as 2003, European data protection authorities have regularly expressed concerns about Whois.¹ Despite a number of efforts to update Whois policy and design solutions that meet privacy needs while preserving access for legitimate purposes, the system has remained relatively unchanged. The impending entry into force of the GDPR on 25 May 2018 has created a greater sense of urgency for completing a reform, both within the ICANN Organization and the ICANN multistakeholder Community.

Specifically, since ICANN60, a process for bringing Whois into compliance with GDPR led by the ICANN Organization has dramatically accelerated. The ICANN Community has been called to make proposals and comment on suggested models often with very short time frames for response.

In this process, a number of concerns have emerged for governments:

- the risk that WHOIS may not be maintained to the greatest extent possible, contrary to prior commitments and previous GAC advice;
- Data elements that are critical for legitimate use by the public and third parties (such as Name and Email of a Registrant) would become hidden, without appropriate justification;
- No solution has been proposed for appropriate access to non-public data until a yet-to-be designed accreditation program is implemented, which puts cybersecurity and law enforcement efforts into jeopardy;
- The need to clarify the role of the GAC on which ICANN seeks to rely to define accreditation programs for law enforcement and other legitimate third parties (IP Rights, cybersecurity, etc.).

¹ Article 29 Working Party Opinion on the application of the data protection principles to the Whois directories (13 June 2003), [Letter from the Article 29 Working Party to ICANN](#) (22 June 2006) calling for privacy enhancing ways to run the Whois directories; [Letter from the Privacy Commissioner of Canada](#) (12 July 2006) related to the purpose of Whois and meeting the needs of law enforcement through a tiered approach; [Statement of the Article 29 Working Party on the data protection impact of the revision of the ICANN RAA](#) (6 June 2013) and [follow-up letter](#) (8 January 2014)

GAC Action Required

1. Assess ICANN's recent and future proposals against public policy imperatives, including those spelled out in the [ICANN60 Abu Dhabi GAC Communiqué](#) (referencing the [2007 GAC Principles on gTLD Whois Services](#)), the 29 January [GAC comments](#) on [proposed compliance models](#), and GAC feedback on the [interim model](#) introduced by ICANN ahead of ICANN61 (8 March 2018);
2. Determine the approach the GAC should take to shaping the proposed interim model, including through dialogue with the ICANN Board, GAC Advice, or other possible channels;
3. Consider the role the GAC should play in the design and implementation of an effective compliance model and accreditation system.

Current Position

- [ICANN60 Abu Dhabi GAC Communiqué](#) includes advice in 4 areas related to Whois and GDPR (Section VII.3):
 - Continued relevance of the [2007 GAC Whois Principles](#)
 - Accessibility of Whois for recognized users with legitimate purposes
 - Lawful availability of Whois data for the needs of consumer protection and law enforcement, as well as the public
 - Involvement of the GAC in the design and implementation of any solution and the need for transparency of ICANN in this process
- [29 January GAC Comments](#) on the proposed interim models for compliance with GDPR include:
 - Highlights of ICANN's retained law firm's legal analysis supporting ICANN's goal to maintain the WHOIS to the greatest extent possible
 - Concerns and disagreement with some conclusions of the legal analysis relating to hiding the Registrant email and the need for legal process to support law enforcement requests for non-public Whois data
 - A review of each of the 3 proposed models with recommendations
 - A proposed fourth compliance model calling for:
 - a differentiated treatment of natural and legal person's data;
 - longer data retention periods;
 - the development of an accreditation system for all parties with a legitimate need to access non-public data, including mandatory self-certification arrangements in the interim;
 - a strict application of the model to parties covered within the scope of the GDPR, while others would retain an open Whois
- [GAC Feedback on the proposed interim model for GDPR compliance](#) (8 March 2018), also attached to this briefing (Attachement 1)

Background & Recent Developments

Before ICANN60

- During ICANN58 in Copenhagen, the issue of Whois compliance with GDPR was raised by the participation of Data Protection Commissioners² to a [panel discussion](#) (including the GAC Chair) as well as their [meeting with the GAC plenary](#). Then, the PSWG [briefed the GAC](#) on the balance to be achieved between privacy, the needs of law enforcement and public interests in any future Whois, in line with the [2007 GAC Principles on gTLD Whois Services](#).
- During ICANN59, building on work that had been going on in the RDS PDP Working Group (including seeking legal expertise on [data protection and privacy laws related questions](#) previously asked to Data Protection Commissioners), the [ICANN Community started to explore practical solutions to address the impact of the GDPR on the domain name industry and its users](#). The ICANN Org then initiated an [informal ad-hoc volunteers group](#) which met [once](#) without GAC Participation due to coordination challenges, and quickly changed to [an exercise to gather Whois use cases](#) (users, data elements and purposes) for eventual submission for legal analysis.
- On 24 July 2017, the GAC PSWG submitted a set of use cases gathered among its membership and was quickly followed by [Europol](#), the US [DOJ, FBI](#) and the [Internal Revenue Service \(IRS\)](#) and [Consumer Protection agencies](#), among other [community submissions](#).
- On 11 September, ICANN published consolidated input on Whois Use Cases in its [gTLD Registration Dataflow Matrix and Information](#) (updated on 6 November) and [announced](#) the hiring of the [Hamilton law firm](#) to assist with legal analysis, as well as plans to continue engaging with Data Protection Authorities (DPAs).
- On 12 September, the ICANN President & CEO sent [correspondence](#) to the 28 EU DPAs and the EDPS ([sample letter](#)) to share information about the work of ICANN "to understand the effects of the upcoming GDPR on the global DNS [...] and in particular WHOIS." One response is available, that of [Data State Inspectorate of Latvia](#).
- On 4 October 2017, the ICANN Organization held a first [webinar](#) and updated the Community on its engagement plans.
- On 18 October 2017, ICANN [announced](#) the release of the [first part of the independent legal analysis](#) providing a general overview of key concepts in the GDPR and how these concepts relate to gTLD WHOIS services.

² Mr. Johannes Kleijssen, Director of Information Society and Action against Crime of the Council of Europe, Prof. Joseph Cannataci (UN), Mr. Giovanni Buttarelli (European Data Protection Supervisor), Mr. Wilbert Tomesen (Article 29 Working Party)

During and Since ICANN60

- On 30 October, the Dutch DPA [indicated](#) it had ruled that unlimited publication of Whois data by the .amsterdam and .frl New gTLD Registry Operators violates Dutch privacy law, while recognizing that publishing only limited WHOIS-data of private domain name registrants would be in accordance with current privacy laws. This matter was the subject of correspondence between these registries ([9 October](#)) and ICANN ([25 October](#) and [1 November](#)).
- During the course of the ICANN60 meeting, the PSWG highlighted [to the GAC](#) and [to the ICANN Community](#) the critical importance of maintaining access to Whois data for public safety agencies and other users with legitimate purposes, including the general public.
- At the conclusion of ICANN60, on 1 November 2017, in its [Abu Dhabi Communiqué](#), the GAC advised the ICANN Board on this issue (see "Current Position" section above). This advice was subsequently [accepted by the ICANN Board](#) on 4 February 2018.
- On 2 November, ICANN [announced](#) it would defer taking compliance action against registries or registrars submitting a reasonable compliance model. Following this announcement, the GAC drafted and considered additional advice due to concerns with the statement, including the disincentive to find a global solution to GDPR compliance and the risk of creating a fractured or insular Whois system.
- On 27 November, [a joint GAC/ICANN call](#) was organized with a view to facilitate a dialogue prior to further actions being by either party. During the call ICANN described its approach to the matter and highlighted the importance of GAC input in the process. This call subsequently led the GAC to seek further [clarifications](#) from ICANN on 17 December. ICANN [responded](#) on 22 February 2018.
- On 6 December, in a [letter to ICANN](#), the Article 29 Working Party³ :
 - indicated its awareness of current developments, including the 2 November Contractual Compliance Statement;
 - reiterated its position that "*unlimited publication of personal data of individual domain name holders raises serious concerns regarding the lawfulness of such practice under the current European Data Protection directive*";
 - suggested that "at first glance" ICANN and Registries are to be deemed joint controllers under European data protections laws, and that purposes of Whois directories can be achieved via layered access, including access for law enforcement authorities.
- On 8 December, ICANN issued [detailed guidance](#) for submissions of compliance models by the ICANN Community. A total of 5 [community-proposed models](#) emerged since then.
- On 21 December, ICANN [published](#) additional [legal analyses](#) ([Part 2](#) and [Part 3](#)), and sought Community input on the layered access approach proposed to comply with

³ This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy

the GDPR. It also set an aggressive timeline for settling on a compliance model for ICANN by end of January.

Discussion of actual compliance models since the beginning of 2018

- On 12 January, ICANN [published](#) 3 proposed models for review by 29 January. These were discussed between the GAC and ICANN Org on 25 January, in the [second joint call](#). Among other things, ICANN reiterated its call for detailed input from GAC to assist with future regulatory engagement.
- On 29 January, the GAC provided its [comments](#) and suggested a fourth compliance model (see Current Position section of this briefing above). Other [community comments](#) include those of the European Union ([European Commission letter and comments](#) submitted by the European Commission on behalf of the whole of the European Union), the [U.S. Government](#), the [UK National Crime Agency](#), and the [Online Coalition for Accountability](#) (on the specific issue of the Registrant's Email address becoming non-public data).
- On 2 February 2018, ICANN held a second [webinar](#) during which it reviewed and [compared](#) the community input received on the proposed models and answered various community questions.
- On 12-13 February, law enforcement experts participating in the [Intersessional PSWG meeting in Brussels](#) identified specific needs and challenges to be addressed in the implementation of any GDPR-compliant Whois system. An [expert considerations document](#) circulated to the GAC on 16 February, proposed guidelines to support implementation of the necessary features of an accreditation, authentication and access system, including:
 - Permanent law enforcement access to non-public Whois data on a query basis without the need for justification of each individual request
 - Centralization of credentials for accredited users (to be assigned and maintained by one entity)
 - Centralization of access to ensure continued access to data regardless of location of storage, while minimizing the need for international bulk data transfers
 - Confidentiality of law enforcement requests
 - Capability to cross-reference current and historical Whois data
 - Safeguards to ensure accountability and purpose limitation
- On 28 February 2018, after engaging with various parts of the community for a few weeks, including the GAC in the third joint call of 21 February 2018 (Notes forthcoming), ICANN [published](#) a [summary description](#) of its Proposed Interim Model, including considerations of an accreditation program for access to non-public data. On the same day, the GAC PSWG held a first phone call to discuss the model.
- On 6 March 2016 the GAC discussed the model on a dedicated [conference call](#) to consider a [draft GAC Response](#). During that call, it was agreed to submit comments on behalf of the GAC before the start of the ICANN61 meeting, as requested by ICANN.

- On 7 March 2018, ICANN [reported](#) on its engagement with the Article 29 Working Party regarding the proposed interim model. It indicates intentions to discuss in greater details the justification of the model ahead of the next plenary meeting of the Article 29 Working Party in April 2018.
- On 8 March 2018, ICANN [published](#) additional details about the proposed interim model in a so-called "[cookbook](#)". As this was not available at the time of drafting the latest GAC Comments (attachment 1) could not take this information into account.

Document Administration

Title	PSWG Meeting
GAC Brief No.	ICANN61 Agenda Item 21
Distribution	GAC Members
Distribution Date	9 March 2018
Prepared by	GAC PSWG

**ATTACHMENT 1: GAC Feedback on the proposed interim model
for GDPR compliance (8 March 2018)**

Document starting next page.

ICANN | GAC

Governmental Advisory Committee

Distribution	Public
Date	8 March 2018

GAC Feedback on Proposed Interim Model for GDPR Compliance

I. Introduction

The Governmental Advisory Committee (GAC) welcomes the opportunity to provide feedback on ICANN’s Proposed Interim Model for General Data Protection Regulation (GDPR) Compliance.¹ We appreciate the challenges involved in reconciling the many community interests and public policy concerns raised. We were encouraged that “finding a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible [was] a high priority” for ICANN (Nov. 17th Blog², reiterated Dec. 21st Blog³). The GAC is committed to support ICANN and the community in ensuring full compliance with GDPR and discussing the appropriate way forward. The following comments build on prior GAC advice and public comments.⁴

While we recognize that the interim model is a product of balancing the various views of stakeholders, the GAC takes this opportunity to identify where the GAC has concerns, and notes that in many places the model could benefit by taking into account the legal advice provided by ICANN’s own selected legal advisors, the Hamilton law firm.⁵ As noted in the GAC’s prior public comment on ICANN’s three proposed models,⁶ the Hamilton law firm’s Part 3 Analysis expressed the view that:

- ICANN’s Bylaws support the conclusion that the purposes for WHOIS services should serve the legitimate needs of law enforcement and promote consumer trust;
- the processing of WHOIS data for law enforcement purposes (including investigating and countering serious crime, fraud, consumer deception, intellectual property violations, and other law violations) should constitute legitimate interests for processing of personal data under Article 6.1(f) of the GDPR;

¹ <https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf>

² <https://www.icann.org/news/blog/data-protection-privacy-activity-recap>

³ <https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year>

⁴ See e.g., GAC Principles Regarding gTLD WHOIS Services at https://gacweb.icann.org/download/attachments/28278834/WHOIS_principles.pdf; GAC Advice set forth in Abu Dhabi Communiqué at <https://gac.icann.org/advice/communiques/public/gac-60-abu-dhabi-communique.pdf> at pp. 11-13

⁵ available at <https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en>

⁶ GAC Feedback on Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union’s General Data Protection Regulation at <https://www.icann.org/en/system/files/files/gdpr-comments-gac-icann-proposed-compliance-models-29jan18-en.pdf>

ICANN | GAC

Governmental Advisory Committee

- public access to (limited) WHOIS data (including Registrant name and address) should be maintained to the extent possible, and only complemented by layered access where required; and
- Some EU mandated public registries have considered it to be a public interest, laid down in law, to keep a public record of the owners of EU trademarks, company registers, and domains in EU ccTLDs and hence “implicitly stated that such interests overrides the interests or fundamental rights and freedoms” of the trademark registrants.⁷

In the following submission, we 1) list what we support and have concerns with in the interim model; 2) highlight the potential consequences of altering the current WHOIS model in a way that goes beyond what may be required to ensure compliance with the GDPR; and 3) encourage ICANN to consider further refining its approach to ensure that its model balances the important public policy issues involved to the fullest extent possible.

II. Interim Model Analysis

There are a number of positive elements in the interim model that deserve mention. We support in particular:

- the objective of identifying clear purposes for the processing of WHOIS data which include providing a framework to address law enforcement needs;
- the continued collection of full thick WHOIS registration data;
- the requirement for registrars to transfer all collected WHOIS data to registries and data escrow agents;
- the GAC's role in advising ICANN and the community on potential accreditation systems and codes of conduct for access to non-public WHOIS data by users pursuing legitimate purposes including law enforcement and others (such as cybersecurity researchers, intellectual property rights holders, and consumer protection advocates, among other groups);
- maintaining the current data retention requirements;⁸
- that any future accreditation system will provide for full access by law enforcement agencies;

- that ICANN-approved dispute resolution providers (e.g., under the UDRP or URS) would have full and real-time access to WHOIS data for case administration purposes; and
- that any future accreditation system will maintain anonymized WHOIS queries.

⁷ See <https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en>

⁸ Historic WHOIS data is very important for investigating illicit conduct and relied upon by law enforcement and other user groups for legitimate purposes.

ICANN | GAC

Governmental Advisory Committee

On the other hand, the GAC has a number of concerns:

Although ICANN's proposed interim model takes preliminary steps towards a GDPR analysis, the model does not yet fully assess which data elements are needed, including the proportionality of disclosure to the public, why the masking of certain information is justified, and the details regarding access to gated information based upon the purpose and credentialing of user groups. The absence of these aspects make it difficult to assess the data protection compatibility of the ideas put forward. The GAC understands that ICANN plans to publish a more detailed rationale and would encourage ICANN to share this rationale swiftly to ensure that it can be taken into account by the GAC and the rest of the Community in reviewing the proposed interim model.

The interim model indicates that the data set forth below would not be disclosed to the public but does not include an assessment of proportionality. We also note that the Article 29 Working Party has not excluded publication of some personal data, as long as this is justified in light of the legitimate purposes pursued with the WHOIS directory and is based on the legal ground of performance of a contract or the legitimate interests pursued by the controller or by a third party. Accordingly, the GAC would appreciate further details on the restrictions on disclosing the following data elements set forth here.

Masked Information:

- Registrant's name;
- Registrant's email;⁹
- name (to the extent they are legal entities, *e.g.*, companies or organizations); and
- Administrative and Technical contact's state/province and country (this position is inconsistent with the model's treatment of Registrant information which permits the public display of State/Province and country)

In this context, the GAC has previously advised that public access to (limited) WHOIS data (including Registrant name and address) should be maintained to the extent possible, and only complemented by layered access where required. In particular, for the Registrant's name and email address, community input has shown that these elements are crucial for achieving a number of public interest purposes, which cannot be met by providing an anonymous forwarding mechanism.¹⁰ A minimum amount of accountability should be ensured, allowing individuals to ascertain whom they are dealing with online. When an even greater degree of privacy is required, privacy/proxy services are available to allow for such privacy while ensuring that there is an identifiable contact person.

⁹ For a discussion of why the Registrant email data field is important, *see e.g.*, Coalition for Online Accountability letter to ICANN re: Importance of Public Access to Registrant Email Address at <https://www.icann.org/en/system/files/files/gdpr-comments-coa-icann-proposed-compliance-models-16feb18-en.pdf>

¹⁰ *See e.g.*, GTLD Dataflow Information and Matrix <https://www.icann.org/resources/pages/gtld-registration-dataflow-matrix-2017-07-24-en> and Final Report from the Expert Working Group on gTLD Directory Services at <https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf>

ICANN | GAC

Governmental Advisory Committee

The GAC also notes that challenges to access to non-public data may still arise for public authorities due to national laws that may require a legal basis permitting access to non-public WHOIS data. Certain countries may require the use of formal and time-consuming mechanisms such as mutual legal assistance procedures to obtain non-public information. Therefore, it would be preferable to pursue solutions where, based on “important reasons of public interest” and examples that exist already in other contexts (as mentioned in Hamilton Part 3), WHOIS information is kept public to the maximum extent possible.

Pending a more detailed analysis based on the additional elements to be provided, the interim model does not seem to maintain the WHOIS to the greatest extent possible in line with ICANN's own commitment and previous GAC advice. In fact, the new proposal suggests significant changes to the WHOIS system, including masking several categories of previously public information. The GAC is concerned that these changes are not supported by the necessary analysis and supporting rationale. The proposed system risks hindering the efforts of law enforcement and other actors in combatting illicit activities and mitigating DNS abuse.

Further issues of concern include:

- the lack of clarity for the guaranteed full and real-time access by WHOIS users other than law enforcement pursuing legitimate purposes during the interim model and any period preceding a temporary stop-gap accreditation system;
- masking information related to legal persons from the public¹¹ despite the fact that the GDPR does not apply to them, and the example of the .amsterdam registry showing that there is a feasible way to distinguish legal from natural persons;¹²
- the lack of clarity regarding the period between the implementation of the interim model (May 25th) and the finalization of the mechanisms that are to be implemented to enable a layered access to some WHOIS data, such as accreditation programs. In particular, the GAC is concerned that during this period, access to important WHOIS data will be impossible if no “interim” measures are designed and implemented;
- the lack of a *required* temporary system that provides a channel for law enforcement and other third parties to access non-public WHOIS data. This would essentially let crucial WHOIS data “go dark” for an undefined period. As a consequence, these WHOIS data would become unavailable for investigative and mitigation efforts aimed at curbing DNS abuse and combatting illicit conduct. Once a significant portion of WHOIS becomes unavailable to the public, the proposed model does not *require* contracted parties to adhere to a temporary

¹¹ 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. This represents a significant overreach in terms of ICANN's stated goals to be in line with GDPR. Regarding ICANN's comment that registrations of legal persons may contain personal data of natural persons, respectfully, this is a determination made by the legal person, and can be avoided on their end.

¹² See nic.amsterdam/whois-privacy/

ICANN | GAC

Governmental Advisory Committee

system for law enforcement and third-parties. A temporary stop-gap system to access non-public WHOIS information will be necessary because of the inevitable substantial time gap between adoption of the interim model and the creation and implementation of a new system to accredit law enforcement and other third party users. An alternative to a stop-gap solution would be for ICANN to consult with Data Protection Authorities to explore the option of enforcement forbearance pending completion of an accreditation system;

- the lack of clarity on what if any “limitations” in terms of query volume are envisaged under an accreditation program;
- it is not clear whether and/or how port 43 access (interface allowing for automated queries to get bulk access to WHOIS information directly from the WHOIS server) will be implicated in the model and an accreditation system, including whether and how the ability of conducting bulk queries for legitimate purposes will be impacted;
- the apparent absence of any measures or consideration to improve data quality and accuracy; and
- while the GAC looks forward to work with ICANN and the community on designing and implementing the “interim” WHOIS model, especially as an advisory body with expertise on public policy, the GAC expresses caution about a potentially operational role for the GAC for a future accreditation system for law enforcement and third parties. This operational role, which is suggested by the documents published February 28th, seems incompatible with the scant staff and few financial resources of the GAC, which remains an advisory body. However, the GAC expresses interest in the idea of having each government decide which law enforcement authorities have a legitimate interest to access non-public WHOIS data, and providing ICANN org with such information so that ICANN org can manage the accreditation system for law enforcement agencies. Therefore, we would appreciate clarification on the expectations for the GAC role in accreditation and codes of conduct. Regarding codes of conduct, the GAC cannot work without the assistance and support of the broader community and in many cases, it is best left to the specific non-government user groups to organize and accredit themselves so long as they adhere to agreed upon criteria.

III. Consequences

Given the lack of an in-depth analysis for the various elements of the proposal, it may be difficult to ascertain relevant legal aspects including the data protection compliance of the proposed model. In order to make the best possible compliance case, the GAC strongly recommends providing this analysis as soon as possible.

There is an urgent need to identify and implement a *required* temporary system to permit full and real-time access to non-public WHOIS data by law enforcement and other third parties with a legitimate purpose, pending the adoption of a comprehensive accreditation system. Not providing

ICANN | GAC

Governmental Advisory Committee

such a temporary system would likely cause significant harm to the security and stability of the internet and to the effectiveness of law enforcement, as evidenced by the ample use cases and other documentation provided by the Community throughout this process. This harm would be due to the significant increase in the time and resources it would take to acquire non-public WHOIS information pending the development of a formalized accreditation system. If law enforcement cannot quickly and effectively access WHOIS information to assist in pinpointing who owns or controls a domain, it is the public that will be victimized by conduct that may result in serious, if not life and death, consequences. 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.”¹³ We also refer to our previous advice and comments, as well as to the input provided during the various ad-hoc exercises run by ICANN in this context, for further illustration of the consequences.¹⁴

IV. Recommendations

Consistent with our prior public comment on ICANN’s three proposed models, we recommend that ICANN consider:

- The GAC advice set forth in the Abu Dhabi Communiqué, including to maintain a WHOIS system that keeps “WHOIS quickly accessible for security and stability purposes, for consumer protection and law enforcement investigations, and for crime prevention efforts, through user-friendly and easy access to comprehensive information to facilitate timely action” and keeps “WHOIS quickly accessible to the public (including businesses and other organizations) for legitimate purposes, including to combat fraud and deceptive conduct, to combat infringement and misuse of intellectual property, and to engage in due diligence for online transactions and communications;”
- Swiftly providing a more detailed rationale underlying the choices made in the model, including an assessment from a data protection perspective on the basis of evidence and expertise gathered over the last few months, to respond to the GDPR requirements;
- keeping data related to legal persons in the WHOIS database available to the public in keeping with existing practice endorsed by DPAs;
- providing clarity on what is expected of the GAC as it pertains to accreditation. The GAC welcomes the opportunity to provide guidance on accreditation and codes of conduct consistent with the GAC’s role as an advisory rather than operational body;

¹³ Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defense: Building strong cybersecurity for the EU. Available at <http://www.consilium.europa.eu/media/31666/st14435en17.pdf>

¹⁴ GAC Feedback on Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union’s General Data Protection Regulation <https://www.icann.org/en/system/files/files/gdpr-comments-gac-icann-proposed-compliance-models-29jan18-en.pdf>

ICANN | GAC

Governmental Advisory Committee

- providing temporary accreditation/certification systems that include not just law enforcement, but all users pursuing a legitimate purpose including cybersecurity researchers, anti-abuse firms, intellectual property rights holders and their authorized representatives, consumer protection enforcers and others involved in investigations, crime prevention efforts, combating fraud and deceptive conduct, and due diligence for online transactions and communications;¹⁵
- participation in the temporary stop-gap accreditation/self-certification system being mandatory unless a contracted party would violate local laws in doing so, in which case it could apply for an exemption using the existing conflicts procedure;
- consulting with DPAs to explore the option of enforcement forbearance for a period of time to permit the development and implementation of a formal accreditation system;
- providing clarity on whether and how Port 43 bulk access will be implicated in the model;
- providing clarity that any “limitations” in terms of query volume envisaged under an accreditation program would balance realistic investigatory cross-referencing needs and avoid resort to assessment by registrars on a case-by-case basis;
- providing clarity on how ICANN will technically guarantee the confidentiality of WHOIS queries; and
- providing more clarity as to what the next steps are from a practical perspective before the necessary changes are introduced, to avoid uncertainty and loss of WHOIS data.

V. Conclusion

The GAC thanks ICANN for continuing its efforts to find a satisfactory WHOIS solution that maintains to the greatest extent possible information that is critically important to legitimate users while also being fully compliant with GDPR. The GAC also recognizes the difficult task of balancing the interests of the interested and impacted stakeholders. While noting that time is of the essence, the GAC urges ICANN to take these recommendations into consideration. We also reiterate our availability to participate and support the process of defining and implementing an interim model that 1) fully conforms with applicable data protection rules; 2) addresses the legitimate needs of WHOIS users for access to the necessary data elements; and 3) responds to the needs of contracted parties to obtain legal certainty as to the way forward.

¹⁵ The GDPR recognizes these user groups may have legitimate purposes. See *e.g.*, GDPR Recitals 47, 49 and 50.