PANAMA – GAC: Discussion on GDPR
Wednesday, June 27, 2018 – 09:15 to 10:15 EST
ICANN62 | Panama City, Panama

MANAL ISMAIL, GAC CHAIR: Thank you, everyone, sorry to keep you waiting. And thank you, ICANN for accommodating our schedule that is changing in realtime. So we have [indiscernible] presenting the ICANN's proposed unified access model.

UNKNOWN SPEAKER: Thank you. If we could put the slide to the first -- if we could go to slide three. That's great. Thank you. So we've prepared a set of slides that go over the unified access model, the document and pull out various parts. I will go through this quite quickly, but we're happy to go back to any slides in relation to questions but wanted to have the opportunity to respond to questions and have a discussion with you.

So as you are aware, how we approach access in the tiered system has been under discussion since we start the dialogue around the calzone temporary specifications, on the 11th of April, reiterated expectation to develop some sort of model in order to ensure access.

In preparing this as we have shared, we have also taken into account and reflected the other community discussions and prepared a chart that shows that, so we will continue to track how we're incorporating those various things. The purposes, as we've been talking about over the past days, is really to identify a unified mechanism that recognizes the different eligible user groups that may have different criteria relating to those and safeguards in relation to codes of conduct. This document up for discussion and obviously will incorporate any input including from the data protection authorities.

So the model itself has four elements: Eligibility, process details, technical details, and codes of conduct and as shared yesterday in the cross community and high-interest panel, there is also an internal for the legal certainty around if this kind of model can be functional.

So on eligibility, the categories will seek to really drill down around who would be eligible, who determines the eligibility and how would the authentication be developed. So on the eligibility itself, it's really those who would have a legitimate interest bound by the codes of conduct that would be registry operators and registrars will be required to provide reasonable access [reading]

On who would determine the eligibility, the governments within the European economic area, also, as you know, members of the GAC, identify or facilitate identification of the broad categories of eligible groups.

And one of the dialogues here, there are different categories and really getting a clear definition around those including some areas around historically there may be some ambiguity of what would be a representative body, cyber entities.

There is a discussion, as you know, around how would the authentication requirements be developed, for law enforcement clearly in relation to the respective governments. For private third parties, that is the other categories, we would consult with the GAC to identify relevant both sides with expertise but also in case the GAC don't assist with that, we will be working with the broader community around that, and this goes to the categories, for example cyber research, intellectual property. And the specific user groups would automatically approved for access via the model for the purposes would then be moved forward.

If we focus in on the process details overall, how would the process function. The registry and registrars would be required to provide access to any of the eligible user groups as permitted under their local laws of course. The requester would submit to the approval process required by the relevant authenticating

body after they have signed the codes of conduct and received credential or token.

We're looking at two different options and would like to hear back from people on these two different options, including governments and data protection authorities. One, the authenticating body would direct the user to a centralized credential provider who would grant the credential or token. The other would be that the authenticating body would itself provide the required token or credential to the registry operator or registrar. So each of those models are really worth discussing.

We also intend to get some clarity from the European data protection board on two approaches in relation to scope. I know this is been a conversation over the past days. One would be whether authenticated users granted a query-based access on the level and scope is consistent with the identified legitimate purpose or whether the query based is approved for access to the full WHOIS record and this distinction one we need clarity around.

The document also looks to incorporate transparency requirements, but we are, as you know, seeking additional clarification around requirements around logins, discussion around the costing of this model, and of course the review of the

model itself and the effectiveness over time and the mechanisms around that. The document also then looks at the technical details, slide please.

And this is for example, the tokens or certificates would be used to identify the authenticated users and we are happy to take further questions around that.

The final bucket area of the document really focuses in on the codes of conduct. If I can have the next slide. And these would need to be established to really provide some clarity on the appropriate limitations and the proper procedures for accessing the data and the safeguards that need to be taken into consideration. Our assessment is that each of the eligible user groups had that should be a separate code of conduct. However, that working together with the GAC, the data protection board, the ICANN community, that the codes of conduct themselves should have standardized terms and safeguards that are common across all. And the listing here provides several considerations that would be safeguards to be considered. This is not an exclusive list so part of the discussion is whether there are other items that should be taken into consideration here and agreed upon.

Once the authenticating bodies have been identified, they may or may not develop decisional safeguards on top of those

common, the authenticated users would be required to declare adherence to the code and the authenticating body would be responsible for the monitoring and unfortunately, an area that needs to be delved into deeper. High level overview, just as a reminder, if you have any suggestions or ideas, please send those to us at the GDPR at ICANN.org. It gives us an opportunity to post them and take those into consideration as we're moving forward, in addition of course to the dialogues we are having here.

MANAL ISMAIL, GAC CHAIR: Thank you, very much, Theresa, and let me open the floor for questions or discussions. I can see India, please.

INDIA: Thank you. Rahul for the record. My question is for Theresa. If you could take us back to the slide, [reading] there would not be a central repository WHOIS data from which access would be granted. Could be elaborate on this? And possibly John could pitch in and add to the motivation and the reasons why this has been kind of added or included?

UNKNOWN SPEAKER: As you know, currently it's a decentralized system. Currently not the proposal to have a centralized repository around that. Now position may shift.

UNKNOWN SPEAKER: And one of the interesting points that you are probably aware, the data is collected from the gTLD at 2500 separate parties, so each of the registrars when the registration comes in for a domain name collect the information for WHOIS as well as other relevant business recommendation, the records are populated from that original transaction. There has not been a proposal yet, not one we could figure out, how to make work where registrant information is somehow collected in a central repository in any way that would change the connection or make the registrant in any way safer. So this is a concern. If we were to try to bring it into a central repository, whether or not that would change anything about the record other than creating more problems as opposed to fewer.

MANAL ISMAIL, GAC CHAIR: Thank you. I can see Indonesia.

INDONESIA: Thank you for the explanation about the response for the GDPR. What I would like to ask is in your work, do you also consider the

centrally-released [indiscernible] after the Microsoft [indiscernible] case where the US law enforcement failed to get Microsoft data in [indiscernible] I would like to know whether this new act, is it one or two months old, is also considered in your work. Because since yesterday we only talk about GDPR, never talk about [indiscernible], thank you.

UNKNOWN SPEAKER: Certainly it's something we will consider. And if it's okay we will take that question offline and try to provide an answer at a later point. I don't think we could reply to all of the information contained in that question in this forum.

MANAL ISMAIL, GAC CHAIR: Thank you, John. Yeah. I have Trinidad and Tobago and Iran, Mr. Morris and then US.

TRINIDAD AND TOBAGO: With respect to to the authenticating body, you mentioned two issues, one the certification and also a monitoring [indiscernible] not only it does the certification body issue the token or certificate but it's also envisioned that that the body will have a role of monitoring and may even seem to enforce if there is an issue where the person is a bad actor, then that body would then be required to either not just monitor but take some action. And

I thought that would be rather -- it might be onerous for such a body if they have to do this exercise. So when you did say it requires further thought and consideration, was wondering maybe what were some of the thoughts and consideration that this particular body would have. Which seems to me a very important issue.

JOHN: Thank you for the question. We think in light of the fact that the authenticating body would be approving the party that had requested to become part of who could access the nonpublic information, that that body would also be in a good role to determine whether that party was continuing to be an authenticating party and whether they were acting within the scope of the code of conduct created in order to govern the relationship for those parties to be able to access that information.

One of the points raised in one of yesterday's forums is whether the scope of an authenticating body's work is actually within what ICANN does, within ICANN's mandate. And so there is some portions of the GDPR which contain information about possible accrediting bodies which may become relevant to this discussion, particularly as the data protection board considers advise they might provide in August or September of this year

and whether those accrediting bodies might become potential authenticating bodies and how they are capable of authenticating and maintaining whether or not they're the right parties to be accessing the information, I think this will fold together as this comes together. Thank you for the question.

MANAL ISMAIL, GAC CHAIR: Iran next.

KAVOUS ARASTEH: Thank you, Theresa and John, for the presentation. Two small questions. One would be about certification to identify the authentication users, how it works. Is it some written terms or criteria or a box that this user should go through that if all conditions are met then the certificate works well and the authentication is confirmed. How it works, if you could explain that. And I would like to know the criteria of that, how it has been prepared. Did you take into account some of the practices that at least as far as the government are concerned, they are using? So what is the basis of that and how it's prepared.

And second is the code of conduct. As we have mentioned several other meetings, as far as the government is concerned.

Sorry, first of all, certification, how it works, how we prepare that and how it is functioning, a box or a model that all the requests

of the users suggest through that and if all the points are checked and confirmed, then authentication is confirmed and the user should be given access? More explanation on the preparation of that box or model, what element you have taken into account, whether you have consulted the government or not.

And the second point is code of conduct. As mentioned in previous meetings, in the government are based on the policy of the governments in general and may be different from the code of conduct of the private sectors or other nongovernmental. I would like to know whether this has also been taken into account. Thank you.

THERESA: Thank you. The questions you are raising on the certification, those are exactly the kind of things we would like feedback on from the discussions. How would it work in practice and how would one operationalize this across the different user groups. So important questions we're looking forward to receiving additional feedback.

JOHN: And on the second question, I think you are right to point out there may be distinctions among the user groups and the code

of conduct. We think there are standard set of terms that would apply across all of the groups in terms of not abusing the system and using it in an appropriate way, doing what you are saying you will do, but also some things that will be unique for some groups differentiated from others.

TAIWAN: Good morning everyone. From Taiwan, for the record. Since the ICANN's [indiscernible] I appreciate your effort into the work so far for the GDPR issue. And I think the unified access model is very important for organization other than authority to indistinct WHOIS for public interest. I suggest that ICANN finalize [indiscernible] as soon as possible. Besides I also suggest the model [indiscernible] consistent for implementation and regarding the eligible user group, as you mentioned on the page, your slide number 5, currently you mentioned the eligible user group includes intellectual property rights holder, [indiscernible] authority, operational security, researchers and the individual. Here I would like to suggest you include two more kinds of user for your consideration. The first one is is the lawyer who assisted intellectual property owner in protecting their own rights. I think they should also be included in the group. The second one is the domain name registrar who passes the foa, stands for form of authorization. And [indiscernible] registrar needs to process foa. I suggest these two kinds of the

user to be included in the eligible user groups for your consideration. Thank you.

THERESA: Thank you, that's very helpful. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you, I have the US next.

US: Thank you. First of all, I want to thank ICANN for taking the initiative for the conversation and to keep it moving, very helpful. I have a couple of questions, maybe a few, bear with me. In the draft discussion document there is a recognition that codes of conduct will be needed for the eligible user groups that were identified. And also recognition that in the model of course registrars, registries, and ICANN will have the ability to have access to nonpublic information. In light of that, any consideration and should there be, that the registries and registrars also had a code of conduct? Because there is the ability of information being misused by those parties as well.

Another question, and you are probably seeking input on this, what is the vehicle for actually advancing this? It's very helpful to have a discussion document, but not clear how this is actually

going to be formally progressed. Also, what mechanisms are available to actually seeing this implemented? I think these are all questions we will probably ask the board later but helpful to know with respect to this discussion document what was the thinking behind that. And I will stop there. Thank you.

JOHN: Thank you. All very good questions. The registries and registrars, depending upon how this becomes part of an obligation to them. So if the uniform access model is approved and either becomes policy or adopted in some other form, could, contain elements through the contractual agreement, also possible to provide some code of conduct, although I don't think that's been considered yet but interesting idea.

In terms of the vehicle for how a uniform access model could be put into place, as you are aware, we've entered into a policy process, the EPDP, now picked up by the GNSO. So the most perfect model would be if the uniform access model, if that moves quickly and the access model were able to to become part of that other a new policy development process but also consideration depending upon timing of how else that could be done. So important conversation with the community.

And as you heard yesterday, there are discussions about whether that could occur with amended specification, new

temporary specification or better set in a policy as developed. Timing of how the uniform access model goes and what the community dialogue leads to I think will in part lead down a path of how mechanism to implement it and also community consensus and legal certainty we have around the model. That would all be important in consideration how the uniform access model could be made part of the contract and part of this important process.

MANAL ISMAIL, GAC CHAIR: Thank you. John. I have Brazil next.

BRAZIL: Thank you Manal, Theresa, and John. This is Thiago speaking, for the record. I apologize in advance if my question doesn't make sense and would ask if possible for you to explain if there is anything based on my question as if explaining to your grandmother.

In the unified access model, seems to me there are different references to different thoughts, public authorities different roles. Authenticating bodies. Accrediting bodies, bodies that would approve codes of conduct, and we've seen references to the role that the GAC would be performing and there seems to be a differentiation between the role GAC members in general

would be called to perform and GAC members from the European Union. So my question is could you perhaps explain what is the role that the GAC as a collective body would be performing in the unified access model and the thinking behind this differentiation between the GAC members from the EU area and GAC members in general.

THERESA: A very good question. And I think part of is is really the role of the GAC overall, especially when it comes to the governmental entities, particularly in the context of law enforcement, there's also governmental entities relating to the intellectual property, international, getting the feedback from GAC important. Because the GDPR specific to the European area. The highlighting of that in the context of GAC also very relevant. Areas where some of the eligible user groupings bridge governmental and private sector side, and that's a conversation where can the government assist us in identifying groups but also the private sector.

Businesses have a strong interest as trying to deal with bad actors online. Where are the right places for all of those groups to go. That's hopefully a little bit helpful to answer.

JOHN: I think that's right, and I think also in these initial phases, in particular in its design, advice from the governments whether about whether we're approaching this in the right way, whether this is something that's useful and what the role of governments should be. Shouldn't be dictated by ICANN but in fact should be provided by the GAC. So in part when we present things like on slide 5 where we say governments within the European economic area would [reading] other ICANN org will engage with other governments, in part these are proposals. We're asking you, is this the appropriate role of the governments in this discussion informing it and the appropriate role as we're building out the model.

THIAGO JARDIM: And then you would hope that the European authorities would be satisfied with the --

JOHN: I guess that goes -- their role also critical in terms of providing us with legal certainty or answering whether they think this is important or helping us test these concepts.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Manal speaking here. I have Switzerland next.

SWITZERLAND: Thank you, Manal, and good morning everyone. Thank you very much, John and Theresa, for this information. I would like to make first a general comment, and I think that the proposal or the ideas floated go in the right direction and you will see from the discussions we will be having here in the GAC how the advice or the communique text goes. And I think it will go in that direction of recognition of this good basis for discussion.

At the same time, I would like to remind ourselves, especially regarding nonusers of this, we have to be -- nongovernment users, we have to be very aware of, important to remind ourselves -- how decentralized or how complex and diverse the user base is. And the limitations, the approach of authenticating bodies on a global basis may encounter. So I think that we also have to have in mind the perspective of the individual user of this WHOIS data and that the access and accreditation has to be workable, scalable, has to be simple, unbureaucratic, lightweight, cost effective, and also very important, accessible and useable at the global scale, that a lawyer who is trying to protect some brands somewhere in a developing economy or in an emerging country really has this access and that we don't create barriers for that use. Because their use is as legitimate as that of a well-organized brand, organization in Europe or in the

US. So I think that's basic for the acceptance and the legitimacy of this effort.

And maybe some consideration could be made on if there is a scale of gray between an authentication approach with an authenticating body and a certain degree of self certification with acceptance of code of conduct and everything, but let's say in this environment of such a granularity, perhaps we have to give some thought to that.

Returning to the key aspect of having a buy-in from the ultimate supervisors of this, the data protection authorities, I would like to again mention the idea of trying to have a very close interaction with the European data protection authorities. And it would be really useful to have them in the process, not only be a part of a letter exchange that really lags behind what we are doing here. And so I don't know, I just put that idea forward. A liaison would be really helpful in this regard.

And finally after all of this, while I wonder if you already have examples of what could be such authenticating bodies user groups that we are already talking about, not from ICANN org itself but also coming from your interactions with the community. Because I would be very interested in hearing that. Thank you very much.

JOHN: I will just start. First of all, thank you for the comments. Very good comments in terms of a criteria for how an accrediting body, what it would look like, an authenticating body. I think we should take the text out of your comment and actually make it part of our evaluation points of how we would look at such a body, very well stated, and I think it's important we try to achieve that, although, it sounds like almost unattainable standard.

In terms of the liaison concept with the European data protection board or authorities, I think that's a great idea if they are willing to do that. We would welcome that, I like your idea, and we will inquire whether that's something that would be possible.

MANAL ISMAIL, GAC CHAIR: Thank you. So I have Guyana, Iran, European Commission, and India.

GUYANA: Let me endorse the comments of Switzerland. Certainly from a developing nation's perspective, this will have challenge when implemented, and in that way, I know it's early in the game but certainly some performance management regime might be something you want to put in. Because [indiscernible] obligated

to go this. Certainly the authenticating body will have responsibility to perform in terms of how long they take to respond, how long the process is. So I think there's responsibility on both sides to ensure this process works.

And then the last question, to make sure this is as agile as possible. Thank you, Chair.

THERESA: To the point of it being agile and the good criteria being elaborated on, any suggestions on approaches toward that would be helpful. The objective is to make this work and work well, if we can successfully put it in place and in compliance with the laws.

KAVOUS ARASTEH: I think interesting comments from our colleague and the eventual likelihood of misuse. Not to expand the question [indiscernible] we have code of conduct, right? [indiscernible] we have information, availability, non availability, nonpublic information, then user information. How are all these monitored? Is there any manual or any automation in the system that if it's misused, there would be a mechanism disable and so stop giving them access? We need to have sort of a diagram of how the process works from the moment the request

is received by users, code of conduct of the users checked, approved, then the request goes code of conduct, question, knows, and then information from the source and then monitoring. At least the importance is the monitoring. If it's its abused, is it disabled momentarily? An alarm that you have misused that or you have no more access? All of these are questions that need to be clarified to be quite sure. The important thing is for the nonpublic information and the misuse of that. Users in country b, registrar in country c -- all ensuring it's going in proper direction and not used. Because these are the critical issues and it's the heart of the public policy issues and we have to be quite sure that the mechanism works properly. Thank you.

THERESA: Thank you. I think part of the dialogue is exactly to this point of how do we address these points and make sure it's working properly and that the authenticating bodies can play the role in the right way.

JOHN: Part of that -- if I understand the question, part of that is making sure there are clear pathways, an understanding of how it works, transparency of the process, that we can see the flow of

information of the information and the accrediting bodies. We will strive to make sure it's very clear and in diagrams what it is.

MANAL ISMAIL, GAC CHAIR: Thank you. European Commission next.

EUROPEAN COMMISSION: I also want to welcome the fact that ICANN is continuing efforts towards a unified access model. We think it should be as comprehensive as possible to avoid fragmentation between contracting parties and user groups. I would have a few questions which are in a way also suggestions for deepening the reflection on these points.

The first question is on the categories of users. You have added a category which are individual registrants. I am like to know your thinking about adding the category and how you think you can help individual registrants in the process of getting access to data. Because determining a legitimate purpose for, I don't know, we spoke about the grandmother. My grandmother, for example, is not an easy exercise.

Then I would have a question on the scope of data, that is point 6 in your model. You say you will engage with the European data protection board on two possible options to determine the scope of data that is to the identified user. The model, as it

stands is very much looking at the accreditation authentication aspect. Are you going to also clarify and deepen the access aspect and this idea to have as easy access as possible, possibly some form of uniform access granted to the authenticated users?

And sorry for being long. Last question is on the other models. So yesterday we had a very interesting panel so I knew already about the model developed by the ipr community. I knew about a new model developed by a lawyer. I'm sure you are aware of these, but can we use these models, integrate them to move up and beef up quickly your own model? Thank you.

THERESA: I will take a stab. On the category of individual registrants. Many times you might have an individual user who is seeking to identify where the source is coming from. So whether they're being spammed by something, we've heard cases with regards to in some of the discussion around fake news, the ability to track where something might be coming from, a domain name, so that category. But to your point, how do you define that and put around the safeguards in relation to that.

On the question regarding point 6 of the response to a query, had preliminary discussions and gone back to the working party 29 with questions, and these are areas we will continue to pose

questions, in part because we are getting feedback of wanting full access to the record versus specific areas, so that needs to be clarified as to what is compliant with the law.

You had a question on the access and possible details on that. I didn't quite follow that question, my apologies.

EUROPEAN COMMISSION: On the possibility to have uniform formal access. So now a user is being accredited, identified, it goes for the registrars for credentials and is gets access. It will be on a like bilateral basis directly with the registrar. Will there be a way to have some kind of interface that gives a uniform form of access for the user? Instead of having to go to each and every individual registrar? So is there thinking to develop the model in that direction?

JOHN: I think that's a good proposal or idea, and there has been some discussion around it. I don't think that's fully formed on how that information technology point would look like. And the last question about how the IPC BC model -- and I think it's called the philly special -- we watched those carefully, went through those and tried to implement as many of those points as we could into the model and also created a chart which laid out on the different points where we are consistent or differences

between those models. I believe that will chart is available but if not, we can work to publish it. I'm pretty sure it's on the GDPR page.

THERESA: Yes, the chart is available and we can send a link to Manal and the secretariat and have that circulated.

MANAL ISMAIL, GAC CHAIR: Thank you, Theresa and John. I have India then Egypt then Kavous, and we have a couple of minutes remaining. Please try to be brief.

INDIA: Two short points. While consistent [indiscernible] through these discussions is that more flesh these to be put on the access model. It doesn't take away from the value of what this model has added in terms of moving us forward on this discussion. So first of all, I think I support the point made by my valuable colleague from the US regarding codes of conduct for the registries and registrars, a very important point and we welcome it. Other than that, I hate belaboring, hate to put you on the spot for this one, but there's a need for consistency, uniformity, less bureaucracy, predictability of access. So these are all consistent features running through the discussions taking place

in this area. And even as my valuable colleague from the Swiss government pointed out, the [indiscernible] the whole thing is basically access. The access has to be quick, agile, has to be less bureaucratic, and it has to be there.

And this also -- connecting this with the fact pointed out in the discussions yesterday, Facebook has made 1700 requests, and after only three got back to them. And as pointed out by US colleague, the registries and registrars and ICANN are the three bodies that would have full access to the nonpublic parts of WHOIS data. Now the third point in the technical slide in terms of is this a given at this point in time or still up for grabs? Because the fact that you have included it in your presentation, I want you to elaborate it further, that there is at this point in time no central repository envisioned for WHOIS; is that a given? I would like you to elaborate more on that.

MANAL ISMAIL, GAC CHAIR: Would you like me to take the rest of the questions and you address them at one time? Egypt briefly, please.

EGYPT: I just want to stress one point that maybe some other colleagues have mentioned. With regard to the code of conduct registries and registrars and maybe there should be a look at other groups

as well that might be applicable for a code of conduct if they also deal with part of the data and system proposed. One other major point that I want to make sure it's [indiscernible] for in the model proposed to relates to confidentiality in the use of this access model. I think one especially for public authorities working on law enforcement, they want to ensure the use of this model is fully confidential in terms of the query itself, should be kind of invisible to the registry and the registrar and any entity being proposed for licensing and accreditation. And also when it comes to the monitoring of the model, it's important that public authorities still can make their jobs the way they used to with the WHOIS system that kept all users invisible or confidential in their use of the system. This also relates to the cost element and recovery. Some of the models could -- I don't know of course what options are there, but the payment shouldn't be tied to each query in a way that could identify the entity using or making the query itself.

MANAL ISMAIL, GAC CHAIR: Thank you, Egypt. Iran next.

KAVOUS ARASTEH: Thank you. Briefly, I think a reference made that ICANN will be engaged with the government with respect to this important issue. I would like to ask that ICANN consider an appropriate

[indiscernible] what is the mechanism of that engagement? That is point number one. And point number two would be that there are very many good and positive views has been expressed during this ICANN -- which I call them ICANN Panama GDPR, everything was around GDPR. And also in this meeting. Would you take that into account and there's a possibility that you amend your temporary specification or not? Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you, Iran.

JOHN: I think that's about 20 questions of which we will not remember all or have written down, and part of these are very important for us to collect. Because this is an important discussion not just with ICANN org but with the GNSO and those setting the policies and particularly on issues like the central repository where that's a significant change to the way the WHOIS is currently conducted. That has to be part of the policy process discussion and needs to be brought into the community and taken to the GNSO and thought through with the contracted parties as parts dialogue about how that would work.

It is nearly impossible for ICANN org or the ICANN board to dictate a change that is as significant as that, although we

certainly are looking at all those ideas and trying to think through it.

THERESA: The other discussions around whether codes of conduct should be applied to other entities, very good suggestions, and providing that input into the dialogue would be very useful, assists us in a couple areas. One around legal clarity and ISO, [indiscernible] on the costing mechanism, likewise, it goes a little bit to the points made earlier about how can this be as simple and agile as possible and function in a very agile way, building out a system unified that meets the needs of the eligible user groups with the appropriate accreditation bodies around that that is agile and also most cost effective and how to handle that around that. I think that covers most of the points. I hope.

JOHN: And particularly on the legal clarity. This is the sort of issue that becomes a critical element. Because remember this is a proposal for something that becomes part of a contract and policy. And in order for ICANN to enforce its contract, there has to be a certain amount of legal certainty around how that contract can operate within the laws, whether it's one of the 162 or other laws or the GDPR. And so when we think about how this model employs, how the policy process works within it and

other pieces, how that legal certainty employs will be how ICANN can enforce against it, because we don't have governmental or regulatory authority. Our relationship with the contracted parties comes through contracts. So there is the law and then our contracts. The law will supersede our contracts.

So if I am a registrar in Europe right now and I believe GDPR overrides something that ICANN puts into the contract, I can choose not to do that, cite that law, and the only remedy ICANN has available is courts if a disagreement. So we can withdraw accreditation from registries and registrars when they don't follow the policy within the law if it's questionable, whether it's within the law, we go into dispute within the contracted parties which isn't of benefit to anyone and resources for ICANN to do this.

MANAL ISMAIL, GAC CHAIR: Thank you, John and Theresa. And please, for any unanswered questions, let's compile those questions and share them with Theresa and John and we can have either written responses to make sure all questions are responded to. Thank you.

JOHN: Thank you for the very good questions and comments, very useful, and we appreciate this dialogue very much.

MANAL ISMAIL, GAC CHAIR: Thank you.

THERESA: Likewise, and please know you can provide the comments directly to ICANN at the GDPR. Any feedback, ideas, suggestions are most appreciated. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you all, and sorry for the short break. We need to be back from the break at 10:30. Please be back at 10:30 for the meeting with the board. Thank you.

[END OF TRANSCRIPTION]