ICANN Transcription

GNSO Temp Spec gTLD RD EPDP

Thursday, 05 December 2019 at 1400 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. Attendance and recordings are posted on the agenda wiki page: https://community.icann.org/x/U4EzBw

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page: https://gnso.icann.org/en/group-activities/calendar

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the GNSO EPDP Phase 2 Team meeting taking place on the 5th of December 2019 at 14:00 UTC.

In the interest of time, there'll be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please identify yourselves now? And I do believe Franck from IPC is on telephone only at the moment.

We have listed apologies from Volker Greimann of RrSG, Brian King of IPC, and Georgios Tselentis of GAC. They have formally assigned Sarah Wyld, Jennifer Gore, and Olga Cavalli as their alternate for this call and any remaining days of absence. Alternates not replacing a member are required to rename their line by adding three Zs to the beginning of their name, and at the end in parenthesis your affiliation – alternate, which means you're automatically pushed to the end of the queue.

To rename in Zoom, hover over your name and click “rename.” Alternates are not allowed to engage in chat, apart from private chat, or use any other Zoom room functionality such as raising hands, agreeing or disagreeing.

As a reminder, the alternate assignment form must be formalized by the way of the Google link. The link is available on all meeting invites towards the bottom.

Statements of Interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now. Seeing or hearing no one, if you do need assistance updating your Statements of Interest, please e-mail the GNSO Secretariat. All documentation and information can be found on the EPDP wiki space.

Please remember to state your name before speaking. Recordings will be circulated on the mailing list and posted on the public wiki space shortly after the end of the call.

Thank you and with this, I’ll turn it back over to our Chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. Good morning, good afternoon, good evening. Welcome to the 33rd team call. We will follow work according to agenda we adopted yesterday for two consecutive calls. But before entering into discussion of item 6 of the agenda on authorization provider, I would like to ask staff to put up a slide that we developed simply to visualize how much time do we have on our hand and what issues we should be prepared to consider.

Yesterday we agreed to work towards finalization of the report at January face-to-face meeting. I felt that there was kind of sentiment that we will have much more time. In reality, we won't. Therefore, we put together a timetable and topics that we would like to address in each of remaining face-to-face meetings with the method that we used at the beginning. So, in other words, we look at the text of one building block, then we work towards next meeting by looking into next building blocks as we now see, for instance, on the screen, provide comments. We try to incorporate those comments provided already in the text that we reviewed during the face-to-face meeting, simply making sure that we reach face-to-face meeting the stabilized building blocks and we can do in Los Angeles the conversation of systemic nature as well as doing fine reading of the final report, taking out all redundancies and making sure that there is no inconsistency throughout the text.

I will share with you this slide after the meeting, but what is essential that we really concentrate and make homework that we can progress with this. And also when you're looking into outstanding issues, please think not only from perspective of your [interest] but with knowledge that other groups may think. Please come up with the suggestions that you think may find a common ground that we can examine then and hopefully agree.

With this, I would like to thank again staff for putting together this work timeline on such short notice. We can move to the building block on authorization provider unless there is any opposition to a suggested way forward. I see none. So then let's get back to work.

We got to point 4 and we agreed that sub-point A of point 4 would meet a common agreement, though as staff suggest that this is already covered in logging building block and, therefore, maybe it is not worth repeating it it's here. And sub-bullet B that we tried to reformulate, we managed to get a common understanding, but then it was suggested that this is not the right place for this point and we agreed that it would be reflected in the part of the document where we're talking about geographic coverage of this policy.

So with that understanding, we should go to point 5. I see Margie has her hand up. Margie?

MARGIE MILAM: Good morning. I think this language was intended to cover the paragraph that relates to the balancing test was the act by the authorization provider of assessing the legal basis. So maybe instead of entirely deleting it, just say, "The authorization provider must assess the appropriate legal basis," and then that could pick up [61f, 61e], whatever. The different types, that stuff is covered. I think if you delete it then that isn't reflected in, if you will, the operation of how the authorization provider does its analysis.

JANIS KARKLINS: Yeah, but that is already, Margie, covered in point 3. If you look at the previous point, "The requestor will have the ability to identify the lawful basis under which it expects the authorization provider to disclose the data requested, the authorization provider must make the final determination of the appropriate lawful basis."

MARGIE MILAM: Oh okay, sorry. I missed that. I think you're right. Thank you.

JANIS KARKLINS: I am. Thank you, Margie. Alan?

ALAN GREENBERG: Yeah, I'm still concerned about the reference to protect all registrants where not all registrants are protected by policy law, specifically legal persons.

JANIS KARKLINS: Look, we agreed to delete point B already yesterday. For some reason, it's not reflected in the document.

ALAN GREENBERG: Okay, fine.

JANIS KARKLINS: But also we agreed that this question of geographic coverage, we would look where we're talking about how this policy is applied throughout the world.

ALAN GREENBERG: To be clear, Janis, I was talking about legal versus natural, not geographic.

JANIS KARKLINS: That is another story. That's another Oprah.

ALAN GREENBERG: If the words are gone, it's gone. It's fine.

JANIS KARKLINS: Yeah, it's gone. And also staff suggested to delete that authorization provider must log request because we have a logging building block where this requirement is already spelled out very clearly.

Five. Please also read what staff is suggesting that in the context of further requirements, the EPDP Team needs to consider whether it should be must, may, or should to establish the applicability of following requirements starting from point 5, so please keep that in mind.

Point 5: "The authorization provider should make a threshold determination without processing the underlying data about whether the requestor has established an interest in the disclosure of personal data. The determination should consider the elements." Then the list of elements.

"Is the identity of the requestor clear or verified? Has the requestor provided a legitimate interest or lawful basis in processing the data? Are the data elements requested necessary to the requestor's stated purpose? Necessary means more than desirable but less than indispensable or absolutely necessary. Consider whether less invasive means would achieve the same

goal. Are the data elements requested limited and reasonable to achieve the requestor's stated purpose?"

Then sub points. "Each request should be evaluated individually. Such submission should contain a request for data related to a single domain. If a submission relates to multiple domains, each must be evaluated individually. In addition, each data element in a request should be evaluated individually."

These are elements that have been worked out by a smaller group. Then the last sentence in this paragraph would be, "If the answer to any of the above questions is no, the authorization provider must deny the request, or require further information from the requestor before proceeding to paragraph 6." This is a suggestion of the smaller group to consider by the team.

Caitlin, your hand is up.

CAITLIN TUBERGEN: Thank you, Janis. I just wanted to take the opportunity to provide a little bit more context on paragraph 5 and below. The team may remember that back at the face-to-face in Los Angeles, Alan Woods had walked us through a balancing test framework that he used, and following additional legal guidance from Bird & Bird, Matthew Crossman had volunteered to take that framework and provide a little bit more detail based on the legal advice received. We had circulated that balancing test framework from Alan and Matthew shortly before the ICANN66 in Montreal, but because this deals with what the authorization provider would potentially do, we copied and pasted that text into this building block. So that was

the genesis of the information just for some background. Thank you.

JANIS KARKLINS: Thank you, Caitlin. Eleeza?

ELEEZA AGOPIAN: Hey, thanks, Janis. I have a question under bullet 3, the first sub-bullet, "Necessary means more than desirable but less than indispensable or absolutely necessary." I wonder if the team can define this a bit further. That's pretty challenging language to interpret and to comment. Thank you.

JANIS KARKLINS: Okay. Some of the [org] – take this chance or I should? Please think, somebody from the smaller team. In the meantime, Hadia, please. You have the floor.

HADIA ELMINIAWI: I just wanted to quickly note that 5 as is, is okay but we have to keep in mind that the first two bullets like, "Is the identity of the requestor clear and verified?" That's something that's not going to be carried out by the authorization provider but other entities will make sure of that.

Also, "Has the requestor provided a legitimate interest or other lawful basis in processing the data?" Assumingly, the request would never go to the authorization provider unless the identity was verified by an identity provider. And also the request has all

the required fields in there including the lawful basis for assessing. Whether this lawful basis will be accepted or not, then this is the job of the authorization provider. But again, if you want to keep it as it is, it's fine.

JANIS KARKLINS: Thank you. I think some of the elements here is that there might be somebody might try to forge identity and present erroneous credentials or false credentials. There might be a situation that stated purpose is not acceptable and/or frivolously formulated, which does not stand any criticism or [inaudible]. That's why these elements are put forward in the description.

Let me take now a few who have asked for the floor. That is Mark Sv, Franck, and Alan Woods in that order.

MARK SVANCAREK: Thanks. Two points. I actually had my hand raised on the less invasive bullet but I'll start with the necessary means bullet. This line, "Necessary means more than desirable but less than indispensable or absolutely necessary," that is a direct quote from one of the Bird & Bird memos, which in turn was a direct quote from some sort of UK law opinion. So we can go back in the memos and actually pull out what that's from. This really goes to this argument that we've been having about data minimization. What it means is that just because you could do something in a manner which is more expensive or less efficient does not mean that you are lawfully required to do so.

So, more than desirable, I need it to perform the function. Less than indispensible, it doesn't have to be the hardest or least inefficient way if such a way also exists. That's the exact quote that's not language [morgue].

Secondly, less invasive, I don't think that that is defined anywhere. I think I suggested in a comment that we look back to the use cases back when we were still looking at the user groups, we generated a bunch of use cases. I think those use cases are still valuable even if you dispense with the concept of a user group. You just look at a thing needs to happen, here's how it happens, and those go a long way. We spent a lot of time on those and they define what are the means that are required to achieve the goal, which I think is more helpful than this sort of vague less invasive language. Thank you.

JANIS KARKLINS: Thank you for your explanation, Mark, on this necessary. But on the less invasive, what was your suggestion? Do you want to get rid of it, or what was your suggestion?

MARK SVANCAREK: I think I would get rid of it because it's already covered in the previous bullet, the "Necessary means more than desirable but less than indispensable or absolutely necessary."

JANIS KARKLINS: Okay. So you're suggesting the deletion of that sub-bullet?

MARK SVANCAREK: We can discuss it but I don't see the –

JANIS KARKLINS: Now let's see what others will say. Thank you, Mark. Franck, please?

FRANCK JOURNOUD: On the same issue of what data is necessary – this is undeniably a GDPR requirement, but generally it applies to the data controller themselves. As they want to collect data for legitimate purpose, they have to ask themselves, "Could I do this legitimate purpose possibly with less data?" Here we have an unusual situation where the authorization provider has to ask themselves this requestor, can they reach the legitimate purpose with less data or none of this RDS data? It's a hard question for the authorization provider to answer because, well, they're not in that business so they're not this type of crime investigator, they're not any of those requestors. So they may only have vague notions of what is and isn't necessary for those investigations or whatever it is that the requestor is doing.

That's not to say and therefore, this requirement does not apply. But to Mark's point about going back to our use cases, I think the point of those use cases was to say, "This type of requestor is doing this type of investigation. So this type of investigation, the following data fields, etc." If we're to leverage that into the SSAD, would provide well informed guidance to the authorization provider

to say, “Requestor X asked for these data fields and they do or don’t need them.” That’s it.

JANIS KARKLINS: Yeah. Now, thank you, Franck. You see where this comes from. We had this conversation, the knowledge of human behavior, so we can expect that in many cases. People will think, “Okay, if I pay and if I request then I will ask all contact information possible even if I simply want to send an e-mail.” Here the authorization provider should apply common sense and say if you simply want to contact the registrant and you ask all contact information possible, including address and telephone number and whatnot, ultimately your stated intention is to send an e-mail, so you will get not more than e-mail of registrant provided that there is an acceptable reason for disclosing that information. I think that this formulation also came from this type of conversation.

Alan Woods is next, followed by Laureen.

ALAN WOODS: Franck actually made some interesting points. I’ll go through what Mark and Franck both said there together. The first one is Mark was referring to the UK one. Personally, I don’t know exactly where that came from but I just happen to then go to the ICO site. They have a really good example [inaudible] that are in the ICO. They say that the processing must be necessary. That means if you can reasonably achieve the same result in another less intrusive way, legitimate interest will not apply. So that is a very

good way of putting it that it can be reasonably achieved in a less intrusive manner.

I think Franck's point there about we have to consider that that is technically the controller's point of view and put a pin in the concept of who the controller is, of course. That is interesting because this just goes to the balancing test that it is up to the disclosing entity, the controller, to say as part of the balancing test, do they believe that this can be reasonably achieved in a less intrusive way by the requestor. So, really, what Franck is talking about there is he's saying that we should have these use cases. But I think that's probably flipping it. It should be the other way around. The onus in order to provide the detail that can convince the discloser that their interest cannot be met in a less intrusive manner, that is an onus that is on the requestor.

Use case is suggesting that that onus is on the policy, which is very odd. It should always be – and this is the whole point of the balancing test. It's on a case by case basis given to the people saying, "This is why we need it. This is what we've tried to do. This is why we now have come to you in this instance and we really need to move forward," or again, not taking necessity at its highest level. It would be prudent for us to get this at this point to move forward. Not that it's absolutely necessary but that we have taken all reasonable steps to get it in a less intrusive manner. I think that's the key point that there's reasonable steps taken so that they can get it from us.

Again, I'll drop in the link to the ICO legitimate interest into the chat there so people can read that page in itself. It's short and very to the point.

JANIS KARKLINS: Okay, thank you. I understand then you would like to retain but rephrase the second bullet point, right?

ALAN WOODS: Yes. I think we should retain it, to be honest.

JANIS KARKLINS: Okay. Laureen, followed by Amr.

LAUREEN KAPIN: I am weighing in in support of Mark's comment in terms of the second less invasive means would achieve the same goal. My discomfort is similar to the prior comment expressed particularly from a public safety or consumer protection law enforcement perspective. I find it troubling to have the contracted parties put themselves in the situation where they're going to second guess whether some other means would be less invasive. For example, for law enforcement, there could be other means but they may take longer, they may make the investigation less effective, it could create a variety of problems that really a registrar or registry may not know about and it's really not equipped to second guess. So I think eliminating that bullet but keeping the first one which does allow the data minimization principle to be implemented would meet this data minimization goal but not run the risk of having this troubling second guessing by a party that is probably not in the best position to do so.

JANIS KARKLINS: Okay. Here I'm asking – maybe staff can look quickly to the building block on requirements by requestor. Maybe we can add, if there is none in that building block, a general statement that requestor should not put request if less intrusive measures are available, something like that. Flip it around, suggesting that that is not decision of authorization provider but that would be kind of obligation or duty of requestor to see whether they cannot do it in other way. Would that be something, Laureen, you think could fly?

LAUREEN KAPIN: I would need to actually see the specific language to digest it.

JANIS KARKLINS: Yeah. Since we have now a divergence of opinion on this particular point, I'm thinking loud what would be the possible alternative listening argumentation one side and another.

Let me go to Amr and I would like to ask Alan and Laureen to lower hands. Amr, please, go ahead.

AMR ELSADR: Thanks, Janis. I think a lot of interesting comments have been made both vocally as well as in the chat. I'm not clear on why we need to define necessary – or I wasn't until we had this discussion because it seems like we're going to need to give some kind of guidance on implementation to how to do this. I appreciate Eleeza's concerns, the concern she raised on whether this is

vague or not. But I really wanted to support Alan Woods's input on this. If there are other less invasive means to achieve the same goal that the requestor is trying to achieve here, this is key to what necessary is here.

I note that Hadia also put in the chat that she quoted the ICO's explanation necessary and linking that to the principle of proportionality. That second bullet there on whether less invasive means are available, this is also central and key to that principle of proportionality. So you can't really hope to be compliant with data protection regulation or recommend policies that are compliant with those regulations unless you observe that principle of proportionality and making sure that we don't fool around with what necessary means in that context. This is also very important.

That's kind of why I'm a little hesitant for us, for this EPDP Team to try to negotiate what is and isn't necessary. That's supposed to clear, as per the regulation for law. So if we start negotiating amongst ourselves which bullets to keep in, which bullets to take out, then we're going to basically come up with a water down meaning of what necessary is, any water down meaning or implementation of what the principle of proportionality is supposed to achieve. I'm not sure how helpful that would be because then we might end up with a consensus policy that is not compliant with GDPR or other data protection regulations. I just wanted to add that. Thank you.

JANIS KARKLINS: Thank you, Amr. I would like to invite to look in the chat. Caitlin just put forward what is in building block A which is request

requirements. That suggests that there's sub-bullet C that we agreed already that "Information about the legal rights of the requestor and specific rationale and/or justification for the request, that is the basis or reason for the request; why is it necessary for the requestor to ask for this data?" which, in a sense, speaks in a the direction that I was asked to seek less intrusive ways. In a sense, what we are willing to say with the second bullet point, simply flipping it over, putting responsibility to requestor, it is already covered in building block A.

Let me take Mark Sv now. Please go ahead, Mark.

MARK SVANCAREK: Sorry, I'm putting my hand down. Thanks.

JANIS KARKLINS: Margie, your hand is up.

MARGIE MILAM: So, Janis, what is your suggestion on that point to consider whether less intrusive means will [have] the same goal?

JANIS KARKLINS: No, what I'm saying, there is from one side there is a request to delete this second bullet point, and from the other side there is a request to retain it. So if the main concern for those who suggested deletion is that, for instance, the authorization provider will decide whether the law enforcement need this information or can get it from other sources, then in order to avoid that

responsibility being put on the response provider, I suggested that we could formulate that that would be responsibility of requestor, making sure that if there is less intrusive ways to get this information, they should not put in the request. Then we found that in reality that is already covered in building block A, which means that potentially we can delete this sub-bullet and leave only the first one.

MARGIE MILAM: Okay. Thank you. I think that makes sense. I would support that approach.

JANIS KARKLINS: Alan Greenberg, Marc Anderson, and hopefully we can move on.

ALAN GREENBERG: Thank you. I think I support it also. What I was going to point out before we got to this point was we already have heard of examples of request for data being made by data protection officers who truly believe that their request is reasonable under all of these terms and had been refused. So part of this is going to be a learning exercise anyway for the contracted parties to understand, to come to the right answer based on data protection law because they're not necessarily going to be the authority on data protection law. But I think what you're proposing is reasonable here. Thank you.

JANIS KARKLINS: Thank you, Alan. Marc Anderson?

MARC ANDERSON: Thanks, Janis. I'm actually fairly shocked, perhaps I shouldn't be, but I'm shocked that a bullet point that says, "Consider whether less intrusive means would achieve the same goal," is objectionable to anybody. This seems like a pretty no-nonsense bullet point here. If the requestor had a less intrusive means of achieving the same goal, they wouldn't submit the request. For the decision-maker, the authorization provider, this also seems like a pretty no-nonsense step for them to go through.

As I recall in L.A., when Alan was given this example, he described that one of the things that he would do is just pull up the webpage for the domain being requested. And if the information being requested was already available and posted on the webpage – and I think Alan noted that this is a legal requirement in some jurisdictions – then he would deny the request because the data requested is already available in other less intrusive means. So, I do not understand why this is problematic for anybody. This seems like an obligation that the controller needs to perform and I think we need to retain this text to be compliant.

JANIS KARKLINS: Okay. Thank you, Marc. Now, Mark Sv?

MARK SVANCAREK: Thanks. Here's my reasoning. We already have some language in the first bullet, so what you have is necessary, here's what

necessary means. That language came from some legal opinions. Experts in the law wrote that language. Now we have this next bullet which seems redundant to me, it's already covered in the previous things but it's something that we came up with here which has less authority than the bullet above it. I don't think it helps and I think it has the potential to just confuse people what is less invasive. I don't know your use case but this feels less invasive.

We've already discussed it in the previous bullet what is necessary. I get why it feels like we're being evasive by asking it to go away, but that's my reasoning. We already have language that is sort of authoritative and it doesn't add anything and it adds to the risk of variable interpretations. That's my reasoning. Thanks.

JANIS KARKLINS: Okay, thank you. I will take Margie but then I will make a proposal. Margie, please.

MARGIE MILAM: Sure. I think I was going to add on to what Mark was saying. Also that bullet doesn't even track what's in the ICO language, as Hadia pointed out, the proportionality and even the less intrusive, it also adds the element of reasonableness. I don't think it's appropriate to pick and choose the language from that, and so that's why I support removing it altogether.

JANIS KARKLINS: For the moment, there is divergence of opinion, whether we retain or remove this. It seems that there is still a wish from contracting parties' side to have some leverage if like Marc Anderson suggested that if the e-mail address is requested and after simple verification it turned out that e-mail address is posted already on the website and is available, so then that test would not be performed and request will be rejected.

So, for the moment, simply not to waste further time, I would suggest that we put second bullet in square brackets and I will come back with a proposal during the next meeting, simply when we will clean up leftovers from the text. Otherwise, apart from the second bullet point, I did not hear any other comments on any other elements of this point 5 and I take that the rest of the text is acceptable except the second sub-bullet in bullet 3. Am I understanding correct? Okay, we will come back to the sub-bullet. Franck?

FRANCK JOURNOUD: Yes. Again, to the point that I made earlier that for the authorization provider, whoever it is, to evaluate request and necessity, the usefulness of the … whether it's limited or reasonable to the stated purpose of the requestor requires expertise that they won't have. So we need I think in the request building block to develop this on the basis of use cases, that would provide the guidance that the authorization provider can then use to say yes or no.

JANIS KARKLINS: I would not like to accept a blunt form or statement that there will not be expertise. We don't know. And I hope that whoever will be authorization provider, if they do not have internal expertise, they will buy this expertise from outside. They will put competent people or most competent people to deal with this request because a [hell] of money is at stake. So I think we should not prejudge what will be until we do not know, but what I'm absolutely in agreement with you, that policy should be absolutely clear what needs to be done. That I think we're trying to do our best and we will have the reread of all building blocks and we will do a fine reading of the initial report, and then we will try to catch all [inaudible] out of the text.

With this understanding, I would suggest to move to point 6 which reads, "The authorization provider must evaluate the underlying data requested once the validity of the request is determined under paragraph 5 above. The purpose of paragraph 6 is to determine whether the paragraph 7, meaningful human review is required. The authorization provider's review of the underlying data should assess at least…"

And then come bullet points. "Does the data requested contain personal data? If no personal data, no further balancing required. If the requested data contains personal data, does the data originate in the European Economic Area?" With the two bullet points note that for Phase 1, if you have no [report], contracting parties may define between registrants based on geographic location but not required to do so. And contracting parties may also consider whether the requested data originates from any

other jurisdiction with applicable privacy laws that might impact disclosure.

Next sub-bullet point, "If non-EEA data, no further meaningful human review requested."

Then next bullet point, "If the requested data contains personal data and originates in the EEA, the authorization provider should apply the balancing test in paragraph 7 below." Then there was something that is not fully agreed within the group. "If the requested data contains personal data and originates outside of the EEA, consider whether other privacy laws should apply in lieu of the GDPR, such as in instances where there may be conflicts."

This is suggestion of the smaller group what authorization provider should do prior doing manual balancing test. James, your hand is up. Please go ahead.

JAMES BLADEL: Thanks, Janis. Hopefully, you can hear me.

JANIS KARKLINS: Yes, we do.

JAMES BLADEL: Perfect. Thank you. I may be a little behind here but I am struggling to understand how we are making this policy or this particular section EEA-specific. I feel like this has been overtaken by events given the proliferation of and the adoption of data protection laws outside the EEA in other countries including one

that goes into effect here in less than a month in California which will likely and many companies, my company, and I think Microsoft and some other major providers have indicated will be rolled out nationwide in the US. How did we decide that we're going to make this all about the EEA or do we need equivalent paragraphs or other areas including the United States and other countries? I'm just trying to understand why we're focused on the EEA. Thanks.

JANIS KARKLINS: Probably that is our mandate task to start with, but of course we understand that. That's why from the very beginning, we were saying that it would be good to write the standard which could be applied also to other jurisdictions if similar type of personal data protection would come up. But since we are specifically tasked to write the policy for GDPR, that explains why there's a specific reference in EEA. Again, nothing is carved in stone. That's why we are discussing proposal of the smaller group and see where we'll get to that.

Amr is next, followed by Alan Woods. Amr, please.

AMR ELSADR: Thanks, Janis. I just wanted to say that this goes back to the discussion we just had yesterday on whether it would be more desirable to have a uniform policy across all regions of registrants or not, irrespective of whether they are protected by GDPR or not again. So can we just assume that everything we said yesterday has been repeated today and agree that we each will have consensus on treating the registrants differently. Thank you.

JANIS KARKLINS: Before giving the floor to Alan request, whether there is any opposition to the principle that all registrant personal data should be treated in a harmonized manner. I had the feeling yesterday that all of us, we felt that this is the right approach. So if that is so, then of course we should not repeat conversation of yesterday and reword this particular bullet point and make it non-geographically specific. Let me listen to a few observations. Alan, please, followed by Margie.

ALAN WOODS: I just wanted to point out something that Matthew pointed out to me on one of our discussions there. Probably one of the difficulties in paragraph 6 completely, when we sent in the note about the balancing test, we did say that it was guidance for the balancing test as if we were to apply it under GDPR. I don't think it was necessarily meant to go in as a recommendation as to this is how you would apply the balancing test in the EEA as part of a recommendation. We were providing it to give guidance, so to speak, on how a balancing test should be in our minds form for the GDPR. And maybe from that we can distill some meaningful human review type test that would transcend just the GDPR. Again, I am one of the world's worst offenders for making it just GDPR. But in this instance, I think probably distilling good policy from a potential is probably better in this at this point, definitely.

JANIS KARKLINS: Okay, thank you, Alan. Margie?

MARGIE MILAM: I wanted to answer your question. We did discuss this yesterday and I raised reasons why there could be a difference of approaches depending upon where the registrant is. That's why this language, if you take a look at it, it doesn't preclude it's applying outside of the EEA but it merely says consider whether other privacy laws should apply in the lieu of GDPR, and then it also points out such as instances where there may be conflicts. So what I was intending with that language was to give the flexibility there.

For example, if in the US there happens to be a law that requires WHOIS, and we know that there are folks out there that have supported that kind of legislation, then you'd take that into account. If there's a jurisdiction where there is no privacy law at all, you could consider that. So this language isn't prescribing anything specific or requiring anything specific outside of it. It's merely taking a look at it to see if there's something as the rules engine concept, if you will, especially if there's a conflict. We need to have a policy that can accommodate conflicts. That's what that bullet is intended to do. It doesn't prohibit application of the policy broader. It merely says "consider."

Then the other point that I wanted to reiterate from yesterday was that, as we all know, this policy is applied even beyond what GDPR requires because it treats legal entities the same as a natural person. This policy recommendation does not make the distinction that GDPR specified. So I want to be careful in saying that, that this policy covers everything that's required. We've gone beyond that. Where I think it matters is in things like the balancing

test. When you're looking at the balancing test to determine whether to provide disclosure, the fact that someone is a legal entity and the record contains purely information from a legal entity should mean that there should be disclosure. I think that's the reason why I've been pushing for this notion that geography could matter and that might factor into things like how the balancing test is performed.

JANIS KARKLINS: Listening, also your explanation, Margie, maybe what we could do is simply to cluster bullet point 2 and bullet point 3, which are specifically related to European Economic Area in one section with the heading that this is specifically for request coming from EEA. Then the fourth bullet point, we can take a heading for the requests outside or coming outside EEA. Basically, that would mean the rest of the world. Then you have this notion that should consider whether other privacy laws apply instead of GDPR, and then replace or in addition to such as in instances where there's going be conflicts to put them then follow requirements of those privacy laws or something like that.

Sarah, what do you think?

SARAH WYLD: Thank you. Good morning. Just in response to Margie's point, I definitely agree that we need to accommodate a variety of regional laws which may be applicable. We have a set of points to consider in item 7 below, one of which is the legal framework involved. So wouldn't that cover this concern? I would say that we

should rely on that and remove the bullet points that refer to the geographic location entirely. Thank you.

JANIS KARKLINS: Okay. Look, let me then suggest let's look what is in 7 and see whether we can get agreement on point 7, and then we would come back and revisit the conversation about geographic coverage in bullet 6.

Let's see, bullet 7 suggests: "The authorization provider should evaluate at least the following factors to determine whether the legitimate interest of the requestor is not outweighed by the interests or fundamental rights and freedoms of the data subject. No single factor is determinative; instead the authorization provider should consider the totality of the circumstances outlined below." Then comes the list of those circumstances.

Assessment of impact. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing. For instance, triggering legal proceedings.

Nature of the data. Consider the level of sensitivity of the data as well as whether the data is already publicly available.

Status of the data subject. Consider whether the data subject's status increases their vulnerability. For instance, children, other protected classes.

Scope of processing. Consider information from the disclosure request or other relevant circumstances that indicates whether the data will be securely held versus publicly disclosed, made

accessible to a large number of persons, or combined with other data, provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS.

Reasonable expectations of the data subject. Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.

Status of the controller and data subject. Consider negotiating power and any imbalances in authority between the controller and the data subject.

Legal frameworks involved. Consider the jurisdictional legal frameworks of the requestor, contracted party/parties, and the data subject, and how this may affect potential disclosures.

Let me stop here. It's a wealth of information. There are two other points. So far, what's the feeling of the group? Margie, I suspect that this is an old hand that you have up.

MARGIE MILAM: Yeah, old hand. Sorry.

JANIS KARKLINS: Anyone? So these are all elements that should be taken into account and we discussed them in Los Angeles during our meeting when Alan presented his practice.

Okay, next. "If, based on consideration of the above factors, the authorization provider determines that the requestor's legitimate

interest is not outweighed by the interests or fundamental rights and freedoms of the data subject, the data may be disclosed. The rationale for the approval should be documented. If, based on consideration of the above factors, the authorization provider determines that the requestor's legitimate interest is outweighed by the interests or fundamental rights and freedoms of the data subject, the request may be denied. The rationale for the denial should be documented and should be communicated to the requestor, with care taken to ensure that no personal data is revealed to the requestor within this explanation." This is kind of straightforward.

Alan Greenberg? Please, go ahead.

ALAN GREENBERG: Thank you. I'm looking at the word in the sentence saying if it is not outweighed. Should that be a "may" or "must"? The data may be disclosed? That gives the discretion to the person to say, "Yeah, they've made a reasonable request but I don't have to give it out anyway."

JANIS KARKLINS: The data may not be disclosed.

ALAN GREENBERG: No, no. We're looking at the paragraph –

JANIS KARKLINS: Oh, may be disclosed, yeah.

ALAN GREENBERG: Should it be “may” or “must”? Are we giving discretion to the provider to say, “Yes, it’s a reasonable request but I won’t disclose it anyway”? That’s what “may” says.

JANIS KARKLINS: Yeah. Thank you for asking question. Any preference? Alan suggested to put instead of “may,” “must.” Any objections? Mark Sv?

MARK SVANCAREK: Yeah. It’s just a very troubling situation. It’s appropriate for us to say that the decision is made by the controller and then that will be based on factors that are not visible to the requestor. Then having made that decision, they may still decide not to disclose it. Of course, since the balancing test, what went into it and what their reasoning is, there’s really no way to know whether we’re in this contradictory situation that Alan says where they’ve said, “Yes, this is perfectly legit but I’m still not going to do it,” for whatever reason [inaudible] or something like that.

So it feels like we don’t really have a workable policy unless it’s a must, but I don’t see how you can enforce it because everything is obscured from the requestor anyway, right? I don’t know. I’m just very concerned about the situation that we’re in from a policy perspective. Thanks.

JANIS KARKLINS: Okay. You're not objecting Alan's proposal replace "may" with "must"? That's a good thing. Is there anyone against that? Alan, you should not be against your own proposal.

ALAN GREENBERG: No, I wanted to answer Mark's question. But I'll wait until you're finished.

JANIS KARKLINS: No, no. Please go ahead.

ALAN GREENBERG: Most of what we're doing is not testable other than by complaints and audits. So all of this is being done in private and may be logged but logs are not necessarily available. So, yes, saying "must" we can't enforce it other than by normal means of complaints and occasional audits, if they're ever done. I think that applies to an awful lot of what we're doing. I don't think this particular point is unique. Thank you.

JANIS KARKLINS: Okay, thank you. I see no oppositions to change "may" to "must." "May" is deleted and replaced by "must."

JAMES BLADEL: I'm sorry, Janis. James speaking.

JANIS KARKLINS: Yes?

JAMES BLADEL: There are several oppositions in the chat, so I don't know when you're saying there's no opposition.

JANIS KARKLINS: Sorry, I'm trying to multitask but not necessarily I'm successful all the time. Please raise your opposition.

JAMES BLADEL: I was simply pointing out that there were several folks advocating to retain "may" versus "must" in the chat. So perhaps we need to get them in the queue speaking so that their opposition is noted. Thanks.

JANIS KARKLINS: Sarah, please.

SARAH WYLD: Thank you, yes. And thank you, James, for catching that. My hand is raised to say I think it should remain a "may." I agree the data will likely be disclosed after this evaluation is done if, based on this consideration they determined that the interest is not outweighed by data subject's rights and freedoms, but it should remain at the discloser's discretion, and so it should remain a "may." Thank you.

JANIS KARKLINS: Why? Could you explain why?

SARAH WYLD: I think they're just too many individual circumstances to take into account to say that it will always need to be disclosed after, even if all of these things are outweighing their data protection rights. For example, if it is reasonably available elsewhere, like say they wanted to contact the domain owner that's the purpose for the request, and indeed the domain owner can be contacted by using the publicly available information, all of these different factors might be acceptable and yet still the response should be, "No, I'm not disclosing because you can achieve that in a different manner." Thank you.

JANIS KARKLINS: Okay, thank you. Mark Sv, followed by Franck and Laureen.

MARK SVANCAREK: Thanks. To Sarah's point, I think we already established earlier on that the legitimate interest is not established if there were some other method of getting the data, so that particular example I think doesn't hold. So the legitimate interest would be outweighed if it had been determined that there were some other mechanisms. So this is in the situation where it's already established that the requestor is entitled – I hate to use that word – but their legitimate interest is a legitimate interest.

So all of those objections that I think are being put up have already been set aside by the time we get to this bullet, and then we get to this situation where if the term is "may" then there's no recourse at all. You can't even send it to Compliance, right? Because they'll look at this and say, "Yeah, may," and then that's it. Now, it just goes down the hole and there's nothing to do about it. So, I remain concerned about "may."

JANIS KARKLINS: Okay, thank you. Franck, please.

FRANCK JOURNOUD: Unless we enumerate and explain and agree on other grounds that may exist for denying a request – so we're providing a whole sort of criteria, reasonable expectations of the data subject, data necessary, etc., and then we're saying, but you can also deny for any other reason without stating what those reasons might be, etc., and leaving unfettered discretion then … I mean, I don't see the usefulness of this policy. We need to be clear about why it should be or should not be disclosed.

JANIS KARKLINS: This particular bullet point speaks about the interest of data subject versus requestor. I am trying to find out … this discussion really sounds like discussion in UN where sometimes we can talk hours and hours, must versus may, or should versus could.

Laureen, followed by James and Alan.

LAUREEN KAPIN: Yeah, just taking a step back. I fully appreciate the discomfort and risk of liability that perhaps is driving many of the comments we've heard in favor of "may," because there's a desire there for discretion to make sure that protecting themselves and are making appropriate decisions. That said, if we enumerate, as my prior colleagues have stated, all these factors and then still say you can reject it, then I think we're in a situation where there's no policy at all. We're setting all the criteria and then we're saying, "But it could still be rejected." Unless we have some clear policy saying, "Here's what you need to consider and if these factors are met then the data must be disclosed," then it seems to me that we're taking all this time to set policy but then actually there's no policy at all because of this hidden exception that can be invoked and there's no transparency about that. So I'm very uncomfortable with the situation where we're spending all this time to develop all the specific criteria which then can be rejected for no specific reason. I understand what's driving it but I don't think we're ever going to come to agreement if that sort of gap remains where we're spending all this time to set criteria which then can be rejected.

JANIS KARKLINS: Thank you. James Bladel?

JAMES BLADEL: Hi, thanks. Yeah, I just wanted to weigh in on this particular point and maybe just take a step back from this bullet point. I appreciate

the desire to create a deterministic process whereby if a requestor follows a recipe ABC that they are assured to get outcome X, Y, or Z. The problem is that that's just not the world we live in. I think there's a frustration with contracted parties or with ICANN, but really, it's the governments of the world that put us in this particular situation. We're all trying to muddle our way through it.

My concern is that if we box in a registry or registrar, there's this vision that if they don't follow this policy that ICANN Compliance will come in and whack them on the wrist with a ruler and they'll get in line. But really, what will happen is that the registry or registrar will cite their local data privacy law and they will challenge this policy and all of our work for the last couple of years will evaporate in a puff of smoke. So, it is really in an effort to preserve the validity of this policy. I just want to contradict a little bit of what Laureen was saying. It's really a desire to make the stand up that we have to put these safety valves or these release valves in here so that the entire policy is not at risk for some sort of a legal challenge by making the playing field too narrow for contracted parties taking away their discretion entirely. So I'm strongly advocating for the retention of the "may" versus "must." Thanks.

JANIS KARKLINS: Thank you. Alan?

ALAN GREENBERG: Thank you. I won't repeat everything that's been said before. I understand James's position. On the other hand, if we use "may"

there, it is not enforceable by Compliance. Therefore, that essentially gives carte blanche to someone – when we talk about bad actors here – to simply say, "No, I won't do it." Although I appreciate James's position, there's got to be some process or some words associated with it which allow an audit to be done afterwards and someone to say yes. They didn't disclose it even though the balancing test was met, but here is the valid reason why. We can't just put a "may" there without any qualification because it essentially says this whole policy is not enforceable anymore. Thank you.

JANIS KARKLINS: Look, I think we also need to factor in that this may be no issue if we have a fully centralized system with a central gateway and central point of determination. So then as Sarah said, most likely disclosure will be done and the high probability. But the problem may arise if we have hybrid system where 2000+ points of determination will be established and then this may or most likely will turn into different interpretations. So, that is simply additional element that we need to factor in in this conversation.

Marc Anderson and Mark Sv.

MARC ANDERSON: I think this has been a good discussion. I want to applaud people for really trying to understand both sides of the situation on this one. I raised my hand to make a similar intervention as Alan G. It seems to me one of the concerns I'm hearing is that if it's a "may" then the entity making the decision can just carte blanche, make a

no determination without providing any reason. The language goes on to provide rationale for why for the approval, but perhaps similar to what Alan G suggested, one of the ways to help here would be to provide additional language, making the authorizing entity responsible for documenting why the disclosure was rejected, maybe language there documenting why it was rejected and setting some kind of bar to help ensure that this isn't just an arbitrary decision not to disclose and that there is actually just [inaudible] rationale. Maybe that would help bridge the gap between the two.

JANIS KARKLINS: Okay, thank you. Margie? Oh sorry, Mark Sv first and then Margie.

MARK SVANCAREK: Thanks. Marc Anderson, thanks for that intervention. I want to point out, we've been hearing a lot of examples. Maybe this will happen, maybe that will happen. Up above, we have a long list of things to consider. I think James mentioned something about a hodgepodge of laws. I guess I should be talking more loudly. Sorry.

James was concerned that there's a lot of laws and we did add that bullet legal frameworks involved. I think that's a good bullet. I do note that at the end of the paragraph, the rationale for the – that just says the approval should be documented. I assume that the rationale for the rejection should also be documented. But again, it doesn't matter how many bullets we had up above if there's always a ripcord that says, "In spite of all these

considerations, I'm still going to say no," and then providing that rationale and documenting it doesn't actually help. It will be known but there's still no recourse in it. I just don't see how that's going to work in a practical manner. Policy that's based on "please trust us," I've used the "please trust me" argument many times in this policy development process, because I'm Microsoft and you should all trust me, and that really doesn't get me any traction at all and it really shouldn't. Having language in the policy that says, "Most of the time the data is going to be disclosed, but it doesn't have to be." I don't see how it works. So, I just have to keep coming back to that. I'm sorry.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: I wanted to point out a couple things. First of all, we can't ignore that there are bad actors, simply registrars that don't comply. We can't ignore what ICANN Compliance told us in Montreal that they don't have the specificity they need to be able to enforce the contracts. We also can't ignore the current state of WHOIS requests where vast majority of them even when well documented are not fulfilled today. We get responses like, "Go get a subpoena. File a UDRP." That's not everyone, there are registrars that do comply and we're very appreciative of that, but that is the current state today so that's why we're fighting so hard on this. We need specificity that ICANN Compliance can enforce on.

In the "must," to address the concerns that Sarah mentioned, perhaps we could do something like "must disclose," and then maybe have a clause like absent extenuating circumstances and have some ability for the registrars to at least … or not registrars but whoever the discloser is, to go back to ICANN and say, "We can't because…" then ICANN can evaluate whether that's appropriate or not. In other words, make an exception if there is truly this case and make the exception very limited. But to say that across the board, for all requests, it's a "may" instead of a "must" is a very big problem for us. I think we can't ignore what's happening in the current state today.

JANIS KARKLINS: Thank you, Margie. There is a proposal for what Margie formulated now, retain must, but then unless there are other extenuating circumstances. Maybe those who are willing to have "may" may consider this addition that Margie just put forward.

Alan Woods, Alan Greenberg, and Stephanie.

ALAN WOODS: Thank you, Janis. For those of you who follow the program called [drag race], on behalf of the contracted parties, I think we're feeling very attached right now. Just purely because we're assuming that the only bad actors in this space are the disclosing and the contracted parties, whereas what we're actually forgetting here is that a lot of requesters are also very much bad actors as well. There's going to be requesters who will lie blatantly through their teeth and everything that they provide will be the status of the

data subject, the scope of the processing. Everything seems to be aboveboard but there are again – and I think this is where I'm coming into agreement with what Margie is suggesting is probably a prudent approach – that is, that there may be other circumstances which – even though they're ticked every single box, we're still not going to give them the access because as controller, we would still have doubts that that data is going to be misused and that is a breach. Again, to defend the virtue of the CPH, I need to say that. Thank you.

JANIS KARKLINS: Thank you. Alan Greenberg?

ALAN GREENBERG: Thank you. I put words in the chat similar to what Margie suggests. I said, "Must normally be disclosed," then we have a process that must be followed if indeed it's not disclosed.

I agree with Alan Woods. There are bad actors on both sides and yes, you're going to have someone who perhaps, you recognize them as because of abuses that have been demonstrably proven in the past and not just suspected, there may be reasons but those have to be carefully delineated and carefully documented. We cannot give blank carte blanche to not disclose because you don't feel like it. Thank you.

JANIS KARKLINS: Thank you. Please consider proposal of Margie. Simply, time is ticking and I would like to move on. Stephanie, please.

STEPHANIE PERRIN: Thank you. I just want to note that I have been making all my comments in the chat today in the interest of time and I'm a little distressed if it's not being considered because I thought there were a lot of relevant comments in the chat, not just mine, and I don't want to slow us down by sticking my hand up all the time.

In terms of this issue of non-disclosure, surely there must be another mechanism for policing persistent non-disclosure of contracted parties, other than through this SSAD mechanism. In other words, to me, that's an auditable item and in a data trust that I keep promoting, you would be able to go after that to find actors that were not behaving in a way that is consistent with the goals of ICANN. But if you mandate some kind of a heavily intrusive process, where a data controller has to justify turning down a data request, as Alan Woods pointed out in the chat some time ago, it is not a right to get personal data, it's a privilege. I think you're going to have us in court over that. While I sympathize entirely with Margie's proposal and Alan G's, I think that we have to word that rather carefully. Otherwise, we throw a gigantic burden on the contracted parties. Thank you.

JANIS KARKLINS: Thank you. Hadia?

HADIA ELMINIAWI: Okay. Responding to what Alan Wood was saying, in case of bad requesters, liars, or some unforeseen circumstances, why would we go through the balancing test in the first place? All of the other

possible reasons of rejection are considered before the balancing test. Once we're there, we are doing actually the balancing test, I think all of this does not exist. However, I do support Margie's proposal, though I don't find it necessary. However, taking into consideration what Alan and Sarah and others are saying, I think Margie's proposal makes sense. Thank you.

JANIS KARKLINS: Thank you. Alan Woods?

ALAN WOODS: Thank you very much. Noting Matt's [inaudible], I think Matt's comment there about taking this to the mailing list is correct. But I actually forgot to get my actual point the last time. That was, of course, backing office. There is a series of complaints. If you feel that the procedure has not been followed, you can complain. If you feel that the actual application of the law was incorrect, you can complain. This is not a final decision in a way. We've already written this into other building blocks. Let's also think of the other elements which you can rely upon if you believe that the "may" decision or the "should" decision, as Sarah just pointed out, was incorrect in that instance. It's not the be-all end-all here.

JANIS KARKLINS: While I appreciate the conversation, in general, we need to concentrate on the policy recommendations. My question is following all this conversation where "must" was not supported by some groups, "may" was not supported by some groups, so the question is whether we can find some something that would be

helpful. For instance, now I see that there is another proposal to use “should” instead of “may” or “must.” Alan Greenberg?

ALAN GREENBERG: Thank you. Since I started this whole thing, I would support “should” with a qualifying statement following it saying, “If the information is not disclosed, then it must be…” The appropriate logs must justify, explain why. That’s something that can be brought to light, should there be a complaint or compliance action on it.

JANIS KARKLINS: This is already covered by next paragraph where it requires – if the disclosure is not done then the explanation or rationale of denial should be documented and should be communicated to the requestor with the care taken to ensure that no personal data is revealed the requestor within this explanation.

ALAN GREENBERG: The next paragraph says, “If the request is outweighed.” A similar statement here would cover what I’m talking about. The next paragraph has the right words but it doesn’t apply in this case. Thank you.

JANIS KARKLINS: Margie would “should” be acceptable to you?

MARGIE MILAM: No, unless ICANN Compliance confirms they will enforce a "should." If ICANN Compliance confirm that they would enforce a "should" in the policy then I think it would work. But if ICANN Compliance says they can't enforce it, then I think we have the same issue that Laureen discussed.

JANIS KARKLINS: Okay. May I ask ICANN org liaisons either to confirm that "should" is enforceable in ICANN terms right now or bring it back during the next meeting a confirmation from ICANN Compliance.

ELEEZA AGOPIAN: Janis, this is Eleeza. We can go back to our colleagues and come back to you. I just wanted to make one point about that, that assumes that the authorization provider would be either contracted party or would otherwise be subject to an ICANN contract, so it's just something to keep in mind. The language you've been using here makes it sound as though the contracted party is the one who would be the authorization provider. So we can come back to you.

JANIS KARKLINS: Now look, for the moment we do not know who will be authorization provider, we have not decided yet. There are only two options in reality, either authorization provider is a central entity running the gateway or these are 2000+ contracting parties. There's no third option in my view possible. If the central authority is ICANN, and ICANN decides to outsource that to somebody, so that is still ICANN's responsibility under contractual relations

probably. Then my proposal would be we, for the moment, retain "should." Probably if Alan G would agree, we put asterisk with "should" and then we take the sentence from the next paragraph and we put it in a footnote. We would add exactly the same sentence, in case of non-disclosure of data, rationale should be given another also in this paragraph. That would be my proposal and we would confirm it as soon as ICANN Compliance will confirm that "should" is enforceable in ICANN terms. Would that be okay, Alan G?

ALAN GREENBERG: Thank you. I put my hand up to say I think what we need to ask ICANN org is if the contracted party is the party we're talking about making the decision, under what conditions would "should" do they consider should would be enforceable? It's not can you enforce "should" or not, it's under what conditions is it enforceable? If they say under none, that we have an answer that "should" isn't sufficient. If they say it is enforceable, if they document a reason that we can then audit, then it's something we can go ahead. But I agree with Margie, if Compliance comes back and says, "This becomes an unenforceable policy by the use of the word 'should' then we have a problem," so we need to ask them under what condition is it enforceable, if any. Thank you.

JANIS KARKLINS: Thank you, Alan. Eleeza took note on this position that you provided?

ELEEZA AGOPIAN: Yes, thank you.

JANIS KARKLINS: I see Sarah is suggesting to remove something. Look, Sarah, we will do this fine reading and then we will try to remove every redundancy we have in the document. Just for the moment, let's see what we can agree and then we will clean it up. We will come back only to this part of the paragraph. The remaining, I take, is acceptable as soon as we have answer from ICANN Compliance. Let us move to sub-point Eight.

Point Eight is the application of balancing test and factors considering in paragraph 7 should be revised as appropriate to address applicable case law interpreting GDPR guidelines issued by the European Data Protection Board or revisions to GDPR that may occur in the future. Any issue with this statement? I see none. Okay. Let's then go to implementation guidance.

"As noted in paragraph 5 above, in situations where the requestor has provided a legitimate interest for its request for access/disclosure, the authorization provider should consider the following. Interest must be specific, real, and present rather than vague and speculative. An interest is generally legitimate so long as it can be pursued consistent with data protection and other laws. Examples of legitimate interests include: enforcement of legal claims; prevention of fraud and misuse of services; and physical, IT, and network security."

Any issue with this implementation guidance? It refers to paragraph 5, the authorization provider should make a threshold

determination about whether the requester has established an interest in the disclosure of personal data. I see no request for the floor. Then I consider that it's preliminary stabilized. Let us move back to point 6 of this building block, where we had the conversation about laws, GDPR versus other privacy laws.

My question is after now examining or having examined point 7 and basically agreed with provisions of point 7, except this one part should or shouldn't or must, we have the question whether we could separate as now there is typing and make this point more kind of visually clearer that since our task is to speak specifically about GDPR and we're addressing that specific task is given, but then we're also talking about wider scope, knowing that some other countries will come up with a similar data protection law. So we're suggesting that in that case, the response should be consistent with those laws.

Amr, please.

AMR ELSADR: Thanks Janis. This is Amr. I'm not entirely clear if anything's actually changed in the context of addressing whether the personal data originated from the European Economic Area or from somewhere else. The bullet or the sub-bullet under non-EEA where it gives an example of instances where there may be conflicts between a law or a regulation in a non-EEA country with something like the GDPR, for example, I think this should be the focus here. If there are conflicts, then they need to be addressed. But it shouldn't be an example of one of many situations such as if a data protection law is not entirely consistent with GDPR, again,

we're supposed to be recommending uniform policy recommendations that we hope will set a baseline best practices for data protection privacy granted to registered name holders. Again, if there is a clear conflict between the policy recommendations we are developing and the law that is applicable to a registered name holder or its personal data, then sure, that doesn't need to be addressed. But in the absence of conflict, I don't think any of the other stuff should remain. Thank you.

JANIS KARKLINS: Thank you. So you're suggesting that we would extend the GDPR requirements to other jurisdiction except if there is conflict with the existing privacy laws in that country jurisdiction? Is that what you're saying?

AMR ELSADR: If there's conflict with any law in that jurisdiction, actually, not specifically privacy or data protection law.

JANIS KARKLINS: I'm not sure that … Sorry, I'm not a lawyer but there was a case where one of the European courts ruled that the GDPR does not have the universal coverage or power. That is applicable only in the EU and related to EU citizens.

AMR ELSADR: Yes, that is correct, Janis. I'm not disputing that. But I'm saying that we're developing policy recommendations here, which I would hope are based on our understanding of what the practices might be in terms of privacy and data protection regulation or at least the baseline protections we would like to grant registered name holders in the presence of existing regulations such as GDPR. Just because GDPR doesn't affect registered name holders who are not physically located in the European Economic Area or they are not using services provided by a controller or processors that are located there either. Remember, those are also factors.

I'm not saying that GDPR is legally or extraterritorially applicable to everyone everywhere, but we do need to set this baseline here. I'm saying the exception to that recommendation would be if there was a clear conflict between the consensus policies that we are developing and an existing law. Apart from that, I don't think any of the other stuff is necessary or desirable here. Thank you.

JANIS KARKLINS: Okay, thank you. Margie, please.

MARGIE MILAM: I think that what Amr mentioned is actually correct in that you have to look at conflicts broader than just the privacy laws because there may be other laws that come into play that would come into play. I think that that exception should be built into this. The question is whether there's other factors beyond the conflicts that would require or should require a different approach. I think I need to take some time to think about that.

JANIS KARKLINS: Okay. Stephanie, please.

STEPHANIE PERRIN: Thanks. I just jumped in because I believe the case that you're referring to is the recent Google case that is specific to the right to be forgotten. That case found that indeed Google did not need to demobilize its search engines to find something outside of the EU. There are also two related constitutional cases going through the German courts that will most certainly be appealed on the right to be forgotten. The right to be forgotten, of course, is balanced with people's right to know and freedom of information and reputation of political leaders and all of those things. It's quite complex and I'm not sure it's particularly relevant here. Thanks.

JANIS KARKLINS: Thank you. James?

JAMES BLADEL: Thank you. I just want to echo Stephanie's point about the complexities involved here and, of course, laying these requirements at the feet of a small registry or registrar and hoping that they can make sense of it all. I also want to make sure that this group is not putting ICANN in a position where by the text of this calls either explicitly or implicitly, we are saying on behalf of ICANN that some registrants deserve privacy protection and some do not. You should, for example, select a registrar in Europe if you want your data protected because they will do a better job of it

because they have the legal coverage that another registrar doesn't. That playing venue shopping, I guess, at the part of registrants or having ICANN creating an irregular or an uneven regulatory landscape I think opens up a number of other problems including it and not just regulatory or legal problems or compliance problems, but also just a PR problem for ICANN. Thanks.

JANIS KARKLINS: Okay. Look, I think we have a good exchange. If I may suggest specifically on this point 6, two bullet points now are economic area and non-economic area, if you have any specific editorial suggestions how to formulate this paragraph in light of our conversation, please feel free to provide your suggestions in comment area by tomorrow end of the day. Then staff will analyze and try to come up with a new proposal that we could then examine next time we're looking at this building block. It may happen next Tuesday, provided that ICANN Compliance will come back with the answer.

What does it mean? It means that now we have concluded almost everything except we still need to consider the sub-bullet point to speaking about less invasive means then this two bullet points of paragraph 6, and then "may-must-should" issue in point 7. These are the only outstanding issues I consider from this building block. Hopefully, we'll be able to close it completely during the next or one of the meetings. That would be the conclusion. Thank you for participation in this conversation.

Let us move to the next building block. This is on terms of use. On terms of use, could somebody from staff, simply to refresh our

memories because we looked at it sometime ago and then we dropped it for some reason.

CAITLIN TUBERGEN: Hi, Janis. This is Caitlin. I'm happy to refresh everyone's memory.

JANIS KARKLINS: Please.

CAITLIN TUBERGEN: In terms of what you see highlighted in orange, support staff endeavored to take what was originally in the building block, which if you scroll down, you'll see what had been red line before. What we did was we took the overarching recommendation that's at the top and then we put implementation advice for the three types of agreements that are referenced in the original text, which are the terms of use, the privacy policy, and the disclosure agreement. We tried to reconcile but some members of the EPDP Team wanted more specific requirements and others thought it should be a little bit more broad to leave flexibility and implementation.

So we put some of those details in the implementation advice, hoping to bridge the gap between those two schools of thought. The orange highlighted text above is what is currently in the initial report, but as we noted yesterday, because it's highlighted in orange, in this case, it means that this hasn't been reviewed by the team. I hope that helps but I'm happy to address any other questions if there are any. Thank you.

JANIS KARKLINS: Yes, indeed that is very helpful. Thank you very much. Since most likely we have not looked into the text in detail, take into account that we have another 10 minutes on the call to go, I would not suggest going into detailed reading or line by line reading of this text, but simply take a next building block automation. If we could get that on the screen. In the meantime, Marc, your hand is up.

MARC ANDERSON: Thanks, Janis. This sort of maybe a high-level question to maybe help with the review of this language and the terms of use, disclosure agreements, and privacy policies. I guess, on terms of use, I assume we're talking about terms of use of the SSAD system. I think that's what we've talked about. I think that's what you mean.

JANIS KARKLINS: Yes, you're right.

MARC ANDERSON: Then disclosure agreement would deal with the disclosure of non-public registration data associated with requests for that through the SSAD system. I think both of those make sense to me, but I'm not sure I understand where the privacy policy part applies. Maybe somebody has some context on that, I would find that helpful in reviewing this.

JANIS KARKLINS: Alan Woods, do you have an answer?

ALAN WOODS: Well, it's actually more of a support that I think this is to set people up to read this in the sense of a privacy policy is something very specific to the entity, the place for that entity is, who that entity is, who the controller is. I don't think it's really up to us to even define what goes into a privacy policy, it should really be up to the entity to come up with that, we should just literally be saying here, they should have a comprehensive privacy policy and probably bring in an outside counsel or just [inaudible] at that particular time. I don't think we should … I hate to use the term waste time but we would waste time going through what is in the privacy policy, in my opinion, and I think it probably should just be a very simple statement.

JANIS KARKLINS: Okay. That's a good suggestion. That gave us a context for reading this building block. If I may ask to put automation building block. Caitlin, if you could also give us a context?

CAITLIN TUBERGEN: Certainly, Janis. Again, the text highlighted in orange at the top is the text that matches what is in that initial report, Google Doc. Barry, if you can scroll down just a little bit. This text that is below the initial report text had several comments from various members of the EPDP Team. In the initial report text, the support staff endeavored to add in some of those proposed edits and reconcile differences where applicable. The language just appears more

clean and we can all start reviewing from the same point. Again, if there's any questions as to what it used to look like, you can just scroll down into the document and see where those proposed changes are and the proposed edits from the team.

Just as a quick reminder, when you're proposing edit to the initial report text at the top – we noted this in our e-mail and I think everyone has been using this – but please use comments only. Please do not propose edits in red line because it makes it confusing when there's red lines on top of red lines. If you do have questions or edits proposed to this text up here, please mark it up in comments only. Thank you.

JANIS KARKLINS: Thank you, Caitlin, also for reminder of methodology. Any questions about automation building block? If none, then please review those documents, those two building blocks and provide your comments until 8th of December which is next Monday. Is it Monday? Sunday. End of this week, Sunday, which probably for many would mean Friday night. Then support staff would try to factor those in already in the text that we'll be reviewing during the next team call on Tuesday, 10th of December. Our aim would be to close both building blocks as a result of this reading. Then if we're able to pick up those outstanding issues from authorization provider building block, those three elements that we identified, we will do so as well. We have two hours next Tuesday.

With this, I would like to see if there are any questions on the homework. I would like really to encourage make this homework that we can swiftly progress and get through the text. Again, about

the initial report, there are some new elements in the initial report including visual presentation of potential models. If you, by any chance, want to comment those, please feel free to do so because that is important element of initial report as well.

With this, I would like to thank all of you for active participation in today's meeting and wishing a good rest of the day wherever you are. Thank you. This meeting stands adjourned. Thank you.

TERRI AGNEW: Thank you, everyone. Once again, the meeting has been adjourned. Please remember to disconnect all remaining lines.

[END OF TRANSCRIPTION]