ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Tuesday, 10 December 2019 at 14:00 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 of the call are posted on agenda wiki page: https://community.icann.org/x/VYEzBw
The recordings and transcriptions are posted on the GNSO Master Calendar Page: http://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 10th 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?

Hearing no one, we have listed apologies from Greg Aaron of SSAC and Brian King of IPC. They have formally assigned Rod Rasmussen and Jennifer Gore as their alternates for this call and any remaining days of absence. Alternates not replacing a member are required to rename their line by adding three Z's to the beginning of their name and, at the end in parentheses, affiliation-alternate. At this time, you would automatically get pushed to the end of the queue. To rename in Zoom, hover over your name and click over your name. Alternates are not allowed to engage in chat, apart from private chat, or use any other Zoom

room functionalities, such as raising hands, agreeing, or disagreeing. As a reminder, the alternate assignment form must be formalized by way of the Google link. The link is available in all meeting invites towards the bottom.

Statements of interest must be kept up to date. If anybody has any updates to share, please raise your hand or speak up now.

Seeing or hearing no one, if you do need assistance, 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.

With this, I'll turn it back over to our Chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. Good morning, good afternoon, and good evening. Welcome to the 34th meeting of the team. We have the proposed agenda on the screen now. Question: can we follow our propose agenda?

No objections. Thank you. We'll do so. Let me go to the first sub-item. As usual, we're showing you the state of our work. As you see, some blocks have turned yellow, one green, and I hope that we will be able to close today at least two if not three building blocks as a result of this conversation.

With this, I would like to suggest that we go to the building block on the authorization provider. As you recall, last Thursday we had stabilized most of the text. We have three outstanding issues and we agreed that we would address those issues during today's call with the [hope] we would close the building block.

In the run up, we asked team members to [inaudible]. We had received a few comments by last Sunday. As a result, the leadership team worked to elaborate a potential proposal based on inputs provided by the team. You see now the leadership proposal in front of you on the screen. I would like to propose that we work exclusively with those proposed texts and see whether we can converge on those proposals or that we modify them accordingly.

There were a couple of things that probably I would like to raise now, and that is that one input was provided after all deadlines passed and actually when this leadership proposal was already tabled. As a result, of course, we couldn't take that into account in any way. So it would be really good if all team members could follow suggested timelines. Otherwise, it slows down our consideration of the topic. So that's one element.

The second element is that there have been some editorial proposals made over the [agreed-to] text. Again, I do not want to be overly prescriptive, but I think it would be only fair if we would see that all proposals [prior] to the text is stabilized. So it's good that these proposals that have been made or [inaudible] that have been made are really mostly of editorial [inaudible] from one side to another. But, in principle, I think it would be good if we all team members would follow the same methodology that would facilitate

our activities. In other words, provide comments on time and meet deadlines. Then, if there is some editorial suggestions, then put those in comments, not in the text.

With this, I would like to propose that we go to the first sub-item, and that relates to Point – I'm looking – 5, if I'm not mistaken, of the building block. It is about use of the term "less invasive." After receiving and analyzing proposals that have been introduced or suggested by Matthew and [NSG] and Franck, the leadership team recommended that we would maintain the current text, but we would add, in a footnote, a reference to the explanation of what the term specifically means as provided by Matthew. This is in the [inaudible] [row] that you see now on the screen in Matthew's comment.

So that is the proposal of the leadership team. I'm opening now the floor for any comments or rather disagreement on that proposal.

Milton?

MILTON MUELLER: I don't think this is a bad suggestion. I was the one who proposed the rewording for [NTSG], and I guess it should have said, "Would other open, available data sources achieve the same effect?" So, when you say, "Consider whether less invasive means would achieve the same goal," the question of what is more or less invasive is left hanging. I don't think we should spend a lot of time on this. I don't think it's a big deal. I'm fine if we just retain then original language with the footnote.

But I think the point is, if people can go somewhere, like that data-mining source that I pointed to on the list somewhat half-humorously, and get the data without using SSAD, they should. Whether that's less invasive or not is, I guess, not so much the question as to whether it's just easily available somewhere else. That was my point in raising the point originally. If everybody agrees on what we have now, it's fine with me.

JANIS KARKLINS: Thank you. Let's see whether others agree. Margie, followed by Laureen.

MARGIE MILAM: Hi. I don't think language quite gets us to where we need to be. The word "invasive" is not on the ICO website. They use the word "intrusive." They also use it – I put it in the chat – if there's another reasonable and less intrusive way to achieve the same results. So I think we've left out the reasonableness concept. I'm not comfortable with that being something you have to dig through a link a footnote for because I think it won't give the appropriate guidance to the implementation team.

So my suggestion is we change "invasive" to "intrusive" to track what the ICO website says and add the word "reasonable."

JANIS KARKLINS: Thank you. Can we get that on the screen?

In the meantime, Laureen?

LAUREEN KAPIN: Building on what Margie said, we've already discussed in our last meeting the concept and varying degrees of comfort about who makes this decision about their being another means. But what I would add is that, if the authorizing entity is going to rely on this as a basis to not disclose information, then it would be reasonable for that authorizing entity to identify what this other reasonable and less intrusive source is.

Milton, I know that you've said that you referred to the data-mining company humorously, but I would caution that a lot of these data-mining companies – I think Ayden pointed this out in his response – are not necessarily legitimate entities or even engaging in legal actions. You can't necessarily certainly rely on the accuracy of the information. So I would just exercise some caution for how this analysis should be made. It actually needs to be a truly reasonable source that's less intrusive. I would add you should identify that source if you're going to rely on that to reject disclosing the information.

JANIS KARKLINS: Thank you. Now I have James. In the meantime, I would like to ask Margie if the text on the screen is what you were proposing. James, please go ahead.

JAMES BLADEL: Thanks, Janis. I guess I'm fine with "invasive" or "intrusive" and the changed text there. I don't know if my registrar are kicking me under the table, but personally I'm fine with it.

I just want to point out, if I can use one of Milton's good ideas against him right now, that this could be addressed in some respects by development of an appropriate fee structure that attaches cost to use of SSAD. If there's something that's less intrusive, less invasive, more reasonable – whatever – I think the fees of becoming accredited and using SSAD might be a disincentive to abusing this system when other reasonable mechanisms exist for the same data. So I think we can probably solve some of this by appropriately attaching fees to the use of the system. Thanks.

JANIS KARKLINS: Thanks, James. It seems to me that the way forward would be to put in the second bullet point or sub-bullet point or third bullet of Point 5 text which is now seen on the screen: "Consider whether reasonable and less intrusive means would achieve the same goal," and then, in asterisks, but the reference to the URL, giving your definition of the terms we're using.

Is my understanding correct?

It is? So thank you. Then this is our way forward. Now we can go to the next topic, and that topic was related to Point 6. That is about geographic applications. We had a lengthy discussion during the last call. I think we agreed that, in principle, we should try to use the same standard of protection of private, personal data without making a distinction of geography. So we took that into account.

So [my] proposal is to delete the current Sub-Bullets 2 and 3, which point to EEA areas and non-EEA area, and replace those two sub-bullets with the two new sub-bullets, namely, "If required data contains personal data, the authorization provider should consider if the balancing test, as described in Paragraph 7 below, is applicable and proceed accordingly."

The second recommendation would be to commence discussions with ICANN org on the merits of the study to examine the feasibility and public interest and implications of the distinction between registrants on a geographic basis based on the application of GDPR.

So that is the proposal that we would like to put forward for consideration of the group, based on inputs and the conversation we had in the previous meeting.

I see two hands up. Margie and Milton. Margie, please go ahead.

MARGIE MILAM: Thank you, Janis. Actually, I was trying to reply to the previous section. I don't think we addressed Laureen's concern. Laureen asked, if the request is denied because there isn't reasonable, less intrusive means, the decider of that, I think, would actually identify what that is. I think that that's an important implementation guidance to give to the team and include that in the policy.

JANIS KARKLINS: So what then would you suggest? Do you have any specific proposal?

MARGIE MILAM: Laureen, did you have particular language in mind for that? If not, I can help craft something.

LAUREEN KAPIN: Sure, but I think, Janis, Margie just said it, and I said it also. The basis to reject the disclosure request is based on the fact that there's a less intrusive means than "the authorizer shall identify that less intrusive means."

JANIS KARKLINS: Okay. Berry, did you capture that? Could you display that on the screen?

Okay.

[LAUREEN KAPIN]: Okay. [inaudible] feeling.

JANIS KARKLINS: Okay. If you could draft and put it in the chat, we would come back specifically to your point.

[LAUREEN KAPIN]: Sure.

JANIS KARKLINS: In the meantime, I would like to open the discussion on geographic issues.

Milton?

MILTON MUELLER: I don't understand the logic behind the leadership recommendation. Could you put those back up on the screen? It sounded to me like we had agreed in principle that we were going to set a policy that there would be a uniform standard for data protection in the WHOIS system. And there was a recognition, according to that bullet point on the page: it is rare for consensus policy recommendations not to be generally applicable. So that means that we are not geographically distinguishing and that we should have a uniform policy.

So why, if that is the case, are we commencing discussions on a study to examine the feasibility of doing what we said we're not going to do? Why would we want to examine the feasibility and public interest implications of distinguishing between registrants on a geographic basis when we have decided we're not going to do that?

JANIS KARKLINS: Let me explain. The first bullet point captures our idea that we should propose a uniform policy, despite geographic source. The second is, since our exercise is specifically related to GDPR, at least this is our initial task. So then we thought that, while recommending this general applicability, [we'd] see whether any

specifics we need to take into account are based on geography. So that is the logic of the proposal.

I understand you do not like then second bullet point, which is understandable. So [inaudible]

MILTON MUELLER: Let me just clarify the position here. So the position that we're debating is that some of us believe that the policy is that data subjects who register in WHOIS have some kind of protection against indiscriminate disclosure of their personal data and that that right should be protected by our policy, regardless of where they are. Others believe that the opposite, that policy should not be protected and the only reason we are protecting it is because GDPR requires us to in certain jurisdictions. That, of course, is a position that we in the NCSG and I think many others in the stakeholder groups here don't accept.

So it really is a policy choice. It's not a jurisdictional issue. It's a policy choice. That's the point I'm making.

JANIS KARKLINS: Okay. My read of your comment is that you support the first proposed bullet and you do not support the second. You suggest deleting it.

MILTON MUELLER: Yes.

JANIS KARKLINS: Okay. Thank you. [It's clear]. Berry, there is now Laureen's proposed language. If you could capture that while we're continuing talking about geographical issues.

Alan Woods, followed by James. Alan, please go ahead.

ALAN WOODS: Thank you, Janis. As I said there in the chat – this is relation to the previous point about Laureen's point, so I [inaudible]—

JANIS KARKLINS: Okay. Please wait then. James?

JAMES BLADEL: I think I'm just trying to catch up here with the language – there it is. Okay, it's back. I tend to agree with Milton, but for different reasons. I thought that where we left this coming out of Phase 1 is that registrars or registries had the option, depending upon their geography, their jurisdiction, and their market served to make these distinctions, particularly if it was very specific to a limited universe of registrants.

I guess ICANN can study whatever ICANN wants to study, but I think it's very important that we now recommend policies that create different classes of registrants, whether that's based on where they are, the jurisdiction that they operate under, or whether they're legal or natural persons or all these different hair-splitting-type things. The whole purpose of ICANN is to have this globally uniform policy approach. I'm concerned that even

recommending that we set up a feasibility study takes us down the path of creating types of registrants. Operationally, that's very difficult to implement, not to mention expensive. Thanks.

JANIS KARKLINS: Thank you. But you're fine with the first bullet. Alan Greenberg, please?

ALAN GREENBERG: I guess I have some trouble understanding why we're going back and reopening the discussion on geographic and legal versus nature in a discussion on who the authorization providers and what they should be doing. We're opening a can of worms. We're prejudging the issue on legal versus natural, which we are supposed to be having a discussion on this overall Phase 2. I just don't see how we're going to come to closure at this point by trying to build new policy into a section on who the authorization provider is. Thank you.

JANIS KARKLINS: I think that we are going through the process that has been identified and then fine-tuning how the authorization provider should act after receiving the request. That entails different decision points. So now we are at a decision point where we need to consider whether the balancing test is required or not.

The first, if you go to the bullet point itself, says the bigger point is, does the data requested contain personal data. If there's no personal data, then no balancing test is required. But then, if it

contains personal data, then the authorization provider should consider whether a balancing test, as described in Paragraph 7 below, is applicable or not and proceed accordingly because not in every case is the balancing test required by GDPR.

ALAN GREENBERG: Janis, to be clear, I'm happy with that bullet if it stands.

JANIS KARKLINS: At least no one so far has contested that bullet. The second one was proposed to be deleted. This is the one that is proposed now on the screen. So you can support what's on the screen, I understand, Alan.

Alan Woods now, followed by Margie.

ALAN WOODS: Actually, I'm still talking about the previous one, so, again [inaudible]—

JANIS KARKLINS: Okay, sorry. Margie? Let me ask a question. Is there anyone who cannot support the proposal which is now on the screen: to replace in Bullet Point 6 of the building block the two bullets referring to EEA and non-EEA and replace it with the one bullet which is now on the screen ("If the required data contains personal data, the authorization provider should consider whether the balancing test, as described in Paragraph 7 below, and proceed accordingly")? Is there anyone who cannot support that?

Now I have many hands. Those who do not support, please speak now.

So no one speaks. I understand that—

MARGIE MILAM: Sorry. I'm in the queue, Janis. It's Margie.

JANIS KARKLINS: Okay. Margie, yes, please go ahead.

MARGIE MILAM: Sure. A couple things. About the geographic issue, I don't think it's appropriate for us to be rehashing some of the issues that were already resolved. We had already talked about in the past that registrars and registries could make geographic distinctions. So I'm worried that this statement makes it seem as though that's not possible now because that came out of Phase 1.

The other thing is I believe there is a study that Phase 1 recommended … If staff could recall what the subject matter of those studies were, I think that that's something that we were intending to revisit after the studies were done. But I don't remember the subjects in particular. Could Marika or Caitlin identify what the subject of those studies were?

JANIS KARKLINS: Caitlin?

CAITLIN TUBERGEN: Hi, Margie. Thank you for the question. In the chat, I posted some advice from the Board scorecard about the geographical study. I'll just note that it says, "In adopting this recommendation, the Board notes its understanding that there was a divergence in the EPDP about the value of a study to inform the policy and that requests for such a study have been presented to the Board. The Board directs the CEO and org to discuss with the EPDP Phase 2 Team the merits of a study to examine the feasibility and public interest implications of distinguishing between registrants on a geographic basis based on the application of GDPR. Further actions should be guided by the conversations within the EPDP Phase 2 team."

MARGIE MILAM: Okay, but what did our study request relate to? Was it just geographic or was it both that and natural/legal?

CAITLIN TUBERGEN: Thanks, Margie. There were two different recommendations, Recommendation 16 and Recommendation 17. As you may remember during ICANN 66, Karen Lentz from ICANN org made a presentation on the legal versus natural study. So I would recommend going back and revisiting the presentation there if you have questions on legal and natural. What I was pasting in the chat is specific to the geographic study.

MARGIE MILAM: Okay. Thank you. My point though is that this is something that needs further analysis and that we shouldn't jump to a statement that suggests that there would be no geographic distinction until those studies have been completed. I think that that's the outcome of the Phase 1 report and think that we need to continue that work and finish what we had agreed to do.

With regard to the actual language here, the additional concern I had with the language is that it assumes that the balancing test applies in all instances, or at least it seems to. So I just want to clarify that this bullet only applies if the balancing test is applicable under GDPR and that the other bases – contracts and all the others in Article 6 of GDPR – would have their own basis, if you will, and this balancing test wouldn't apply.

JANIS KARKLINS: But this is exactly what this first bullet point suggests, that, if the requested data contains personal data, the authorization provider should consider whether a balancing test, as described in Paragraph 7 below, is applicable or not and then proceed accordingly. If applicable, apply. If not applicable, don't apply. So it's self-evident.

Let me talk Mark Sv, then Daniel.

MARK SVANCAREK: Thanks, Janis. Most of my comments have been overtaken by previous people, so all that's left is just a reminder, when we talk about these sorts of distinctions, to keep natural versus legal separate from geographic distinction. Thanks.

JANIS KARKLINS: Next time, please try to speak slightly louder. This is not referring to legal and natural.

MARK SVANCAREK: I agree, but it was brought up by at least two different people in the discussion. So I just wanted to make sure that we're making that distinction. It's unfortunate I had to make that intervention. Very sorry.

JANIS KARKLINS: Okay. Thank you. Daniel, please?

DANIEL HALLORAN: Thank you, Janis. My point is on Paragraph 6 and 7, not on geographic or legal versus natural. Is that okay?

JANIS KARKLINS: No. After. Then we will go one by one. So, since we're now on this one, let's continue with this one. Thomas?

THOMAS RICKERT: Sorry. I had to get off mute. Hello, everybody. We had a lot of discussions around this in Phase 1, and the ISPCP at the time has already [inaudible] an approach where there's no discrimination of registrants outside the EA because we would potentially give them less rights, less protection, if they were not based in the EA.

Therefore, I think that the distinction that is now being made in the Paragraph 6 artificially creates those two classes of registrants, to some of which certain protections apply and to some of which we only apply balancing tests, if I recall correctly.

So my suggestion would be that we abandon this distinction and that we apply the various legal bases for all disclosure scenarios. If it is 61F, a balancing test would be required. If not, then a different legal basis might be applicable. But I guess, as we create policy that shall be uniform for the domain name industry at a global level – remember, ICANN's slogan is "One World, One Internet" – we should have a consistent level of protection for all registrants throughout the world.

JANIS KARKLINS: Thomas, in the building block, you have in yellow references to EEA and non-EEA. The suggestion is to delete those two bullet points in yellow and replace them with the one which is now on the screen. If the requested data contains personal data, the authorization provider should consider if the balancing test, as described in Paragraph 7 below, is applicable and proceed accordingly." Full-stop. [To the contrary], since last time, we did not agree to discriminate. We are proposing the replacement in the text policy recommendations. So I hope that this is exactly what you were advocating for.

Milton?

MILTON MUELLER: Unfortunately, that's not exactly what we're advocating for because, when you say the provider should consider if the balancing test as described is applicable, what do you mean, exactly? It should always be applicable. If you're saying it's applicable in some places and not in others, then you're creating some form of jurisdictional discrimination. I think that's just inefficient as well as not the right policy from a normative standpoint. I think what Thomas is saying and what I'm saying and I think what most of us are saying is ICANN should set a policy as to what level of data protection applies to domain name registrants we should enforce that consistently. And that's going to be much simpler because the laws are going to change, the jurisdictional requirements are going to change. So the idea of keeping up with all of that is not what we want to do. We want to have a consistent, uniform, global standard for what kind of protection this data gets.

JANIS KARKLINS: I think, if I understand correctly, the balancing test is applicable if the legal requirement falls under 61F but not necessarily if it is different from 61F. But maybe Caitlin can speak on that.

Caitlin?

CAITLIN TUBERGEN: Sorry, Janis. I was on mute. I wanted to note that you had taken the words out of my mouth and that the leadership had discussed that there may be instances where the 61F balancing test is not

required, and that's under different legal bases under GDPR and perhaps other data protection law as well.

However, I did want to note that, in the event that the 61F balancing test is required, it was would be required across the board. That's what this language is meant to note, that there would not be a geographical distinction. Thank you.

JANIS KARKLINS: Thank you. Stephanie, please?

STEPHANIE PERRIN: I just want to point out that we're melding a couple of things here. I thought, as everyone else has said, that we had agreed that we were not going to do geographic distinction, that we were going to come up with the policy. At the same time, we have to take account of the fact that the GDPR 61F balancing test only applies on one of the legal bases, and we would like to at least be accurate in terms of that law.

However – here's where it gets really confusing – if we're going to have a uniform policy, every other law has some of what I believe I referred to last week as a modality for performing the same balancing test, only the words don't say "balancing test." Asking registrars to make the determination of which jurisdiction uses a proportionality kind of language, which one uses reasonableness, which one uses balancing test, and which one spells it out in a whole lot of intricate causes in their sector [of] legislation is [inaudible]. So why don't we just upgrade to the high level, like any normal organization would, and make a uniform policy?

The other thing I'd like to say is, last week, I believe it was Becky who types in the chat that differentiating on a geographical basis causes competitive interests that would be difficult. ICANN has to consider that in its behavior on this policy. Is it favoring certain jurisdictions that haven't bother to pass data protection law? Thank you.

JANIS KARKLINS: Thank you, Stephanie. We need to try to close the policy recommendation but not go beyond that. So we agreed that we should try to apply policy without reference to the geography of the registrant. So let's then talk about the text that reflects our common policy objective, please, because time is going. We need to do many things.

Georgios, please?

GEORGIOS TSELENTIS: Hello. Can you hear me?

JANIS KARKLINS: Yes.

GEORGIOS TSELENTIS: I don't know if I'm confused, but I think we are trying to do two steps in one. I think, if I was an authorizer, I would do the first step to see what is the legal basis under which I'm going to process the data. If this is going – that my legal basis is 61F – I would go to consider the balancing test. So here we are looking at the second

step without making a clear definition that the authorizer has to first examine the legal basis and then, if, as you say, [inaudible], we can go to the balancing test.

But, for me, we could stay at the upper level. We should say that the authorizer first should clarify the legal basis and then do not go to the details of what this entails for the balancing test in terms of geographical implementation because there are many other things that need to be taken into account on the second step, depending on the legal basis. For example, if the legal basis is respect of the contract, then other things have to be made.

So my understanding – forgive me if I miss understood – is that we are trying to mix the second step with the first step, which is to evaluate then legal basis first. Thanks.

JANIS KARKLINS: Thank you, Georgios. Let me take Mark Sv and Margie.

MARK SVANCAREK: Thanks. I do think that, since the requester has to state what their lawful basis is and, even though this started as an exercise in GDPR, there's recognition that there's going to be slightly different laws in slightly different places, it is likely that they are all going to include the same considerations. There was consent received. There's performance of a contract, and there's legitimate interest. I think that the concept of legitimate interest preexists GDPR. I know it's been used in cases before.

So, even though it may not be appropriate to say 61F, for example, or 61A, if we're going to be saying, "Here's my legal basis for making the request," we might as well use those six categories. I think then then authorization provider will be able to figure it out. I don't think it'll be a nightmare. I think that they will standardize on a GDPR level of thinking. Then they will say, "Oh, yeah. This is very similar to 61A," or, "This is very similar to 61E." If we don't take that approach, then there's really no way for us to state what our lawful basis is.

So I think saying "legitimate interest" is the way to go if we're really concerned about this being GDPR-specific. Thanks.

JANIS KARKLINS: Thank you, Mark. Can I now ask Margie?

MARGIE MILAM: Yes. I think I agree with Georgios said: to really focus on the legal basis and stay away from the geographic issue here because I think that's really what the section is attended to address.

JANIS KARKLINS: Having heard different opinions, would now the text on the screen reflect something we can propose as a policy recommendation?

Georgios?

GEORGIOS TSELENTIS: Maybe there are reasons for doing so, but we are focusing on the 61F. As I said, for me it's a two-step procedure. If I'm an authorizer, I'm looking at the legal basis that the requester is stating as his legitimate interest, if I understand Mark Sv well. Then, based on this, it goes to the second step, which is the assessment based on this legal basis about what has to be done at the second step. If it is 61F, what has to be done is a balancing test. If it is a contractual obligation, then maybe the authorizer has to check whether this is a contractual obligation. So that's what I'm saying.

I can understand that the most difficult case is the 61F. If the leadership took this path, it was to start with difficult ones, and I agree to that. I think what is in the bullet now is correct. But maybe we should put it as a process with two steps. I don't know how this sounds to the rest of the group.

JANIS KARKLINS: Okay. Honestly, I do not know what to do. In my view, this is an example of over-engineering that we're trying to do here. Can we get the text of the building block on the screen?

We have Point 5. That already suggests certain actions that authorization provider should do. This is what we agreed already on. So the authorization provider should identify the requester's identity and then the check on the legitimate interests or lawful basis of the requester. Then they ought to check each request on its own merit and then so on. So here we are specifically saying that, if a request does not contain personal data, then it should not do a balancing test. But, if there is personal data requested, then

there should be as assessment of whether a balancing test is required or not. That is based on legal bases. Then they proceed accordingly. I think that there is a logical flow in these steps that we are talking about. Then, if there is a balancing test needed, we go Point 7 and to the balancing test as described in Point 7. So that is the logic of this building block.

Alan Woods?

ALAN WOODS: Thank you, Janis. I still feel that there might be an underlying difference in what people are saying. Maybe I can perhaps ask a very straightforward question by posing two of the exact same scenarios with one major difference.

If I am a registrant – I live in Ireland, surprisingly – and I have an Irish registrar and, if somebody request, because of the legitimate interest under GDPR, that my data is disclosed, the balancing test should apply. Full stop. That is fine. That is what's currently in the wording at the moment. That makes sense.

I think what I need to understand from other people is in the second, that I do not live in Ireland and say I live in Ghana and I have a Ghanaian registrar. Therefore, the GDPR does not affect me whatsoever. I do not have the right. There shouldn't be a contemplation of a legal basis. I want to make sure that we're all on the same page, saying, in that instance, if I'm Ghanaian, then I should also have the balancing test akin to the GDPR applies to be, even though none of the data that I have is applicable under the GDPR. We're saying that, as a policy for the Internet, we will,

in those instances where, if I wasn't the [EU] or the EEA, that Article 61F would apply, and it will apply that test to my data.

So I just want to be clear that we're all on the same page here. That's what the suggestion is here. That is a baseline. I think the way that it is written and I see that as the way it is written, but I also see how, because we keep referring it to as the balancing test, we keep talking about a legal basis. It's still pigeonholing it in the GDPR. So perhaps we need to focus on distinguishing that we're not just talking about the GDPR. We're talking about creating a balancing test that is like the GDPR, and it is applied regardless of where you are, if that is your legal basis or the disclosure legal basis.

So I just wanted to get that clear. Maybe I made it less clear, but that's where I believe our biggest issue is here at the moment.

JANIS KARKLINS: I can confirm that this was the intention in proposing that one bullet point in place of two bullet points that specifically referred to geographic regions. So that was the intention: to take out any notion of geography and apply the same procedure, whether that is a registrant from Ireland or a registrant from Ghana, because there's no reference to any geographies. But we need really to refer to actions that are compatible with our task. Our task prescribes that we need to write a policy on how to implement GDPR in the WHOIS database or how to apply it. Hence, GDPR requires balancing tests. Other policies may require similar things, but we'll call them slightly differently. Nevertheless, for the moment, our reference is GDPR, and GDPR says balancing test.

So that's why the balancing test is used in the text. So we cannot go beyond that. At least, I do not know how to do otherwise.

Let me take Margie and Mark Sv. Margie, please?

MARGIE MILAM: I think, to address what Alan was suggesting, I think we're reading too much into this section because we do still have the recommendation that allows the registries and registrars to make geographic distinctions and natural/legal person distinctions. That's a recommendation that's being implemented from Phase 1. So I think it's not that simple to say that everyone is treated across the board the same because we already agreed in Phase 1 that that's the way it's going to be treated. Now, obviously we didn't like it, but that's the way it is. From the BC perspective, we didn't care for that recommendation, but that's where we landed and that's what's being implemented.

So I just want to explain that it's not as simple as what Alan is suggesting. This language is fine because this is just dealing with the balancing test, but we do have geographic distinctions in Phase 1 already to a certain extent. We also have to recognize that there may be conflicts. So there is proposals already in the U.S., as an example, that [are floating]. Maybe they'll be passed. Maybe they won't. But there is certainly the possibility that there will be laws that aren't necessarily privacy laws, other laws that point to the need for certain information to be pubic. So we have to be able to have a policy that's flexible enough to accommodate all of that. That's what this language does [as] Step 1, Step 2. So that's why this seems to work for me. But I just want to clarify the

notion that we actually do have geographic distinction based on our Phase 1 report.

JANIS KARKLINS: Thank you, Margie. I think that our task is to develop policy that will overrule Phase 1 policy recommendations. If we will recommend that each registrant, no matter where he or she lives, should be treated in the same way, then that would apply for a registrant living in Ireland or Ghana.

On the last call, we had a very lengthy conversation about this principle. I did not hear anyone suggesting that we should discriminate based on the geographic location of the registrant. So is this what you're now saying? Is this your proposal, that we should discriminate? I'm not asking for an immediate response.

Mark Sv?

MARK SVANCAREK: Thanks. I just wanted to agree with one of the points that Alan made. Specifically, he mentioned that we can think of this as creating a 61F-like balancing test. That was the point I was trying to make earlier, that, for all the bases in GDPR, we will be creating equivalent bases. That's what we put forward in our data request – so a 61A-like consent or 61B-like performance of the contract. So his concept of a 61F-like balancing test is what I was trying to get to before. I support that conceptually. Thank you.

JANIS KARKLINS: Then maybe we can say either the way—

[MARK SVANCAREK]: From my perspective, balancing test worked just fine.

JANIS KARKLINS: Balancing test …

[MARK SVANCAREK]: It was a balancing test. It's understood to be similar to 61F.

JANIS KARKLINS: Okay. That's much more precise description. So now the proposal is to change two bullet points referring to EEA and on-EEA in the text of the building block and to replace it with this formulation that we have now on the screen. If the requested data contains personal data, the authorization provider consider if the balancing test, similar to GDPR 61F, as described in Paragraph 7, is applicable and proceed accordingly.

Can we stabilize this point in this formulation?

Daniel?

DANIEL HALLORAN: Thank you, Janis. It's not exactly on point, but it's the same language. I'm concerned about the question of if the requested data contains personal data. I'm not sure if that's going to always be immediately apparent to anybody, just from looking at bits of

registration data that contains personal data. I don't know if you could look at an e-mail address and always determine whether or not that is personal data, just from the e-mail address or the phone number or even the name of a registrant. It sounds like we're assuming. We could always look at it. I don't know if that is automatable or if anyone can do that (let's say it's a centralized authorization provider): if they're going to be able to look at just the name and e-mail address and say categorically this is or is not personal data. Thanks.

JANIS KARKLINS: I think we are using standardized language through the text, and that is personal registration data. Maybe we could stick to the same formulation throughout the text. Then that should be understood by default. That is personal registration data.

Mark Sv?

MARK SVANCAREK: I just wanted to ask James for a clarification on the chat. It seems to me he's saying that currently GoDaddy applies a geographic distinction, which means it's practical, I guess. But he's hoping to eliminate that today? Is that what you're saying, James? Could you please clarify? Thank you.

JANIS KARKLINS: James, please?

JAMES BLADEL: My point in the chat was to respond to Margie's comment that some registrars are making geographic distinctions currently under the temporary spec. I think it's no secret that GoDaddy has attempted to apply the temporary spec to registrants, data subjects, that we believe are directly covered by relevant national privacy law. Initially, that was GDPR, but that has since expanded in reflection [to] adoption of data privacy laws in other jurisdictions. So that's a moving target. That's my point, Mark, that making a geographic distinction is not a stab at exercise, where you can just flag something and then go home. You're constantly measuring your exposure in response to shifting privacy legislation, and then universe of uncovered folks is getting smaller all the time. Thanks.

JANIS KARKLINS: Okay. I think that we could [leave] this. In the chat, there was a proposal from Chris that maybe a formulation similar to the requirements under GDPR would sound better than "similar to GDPR 61F."

Can we follow up on Chris's suggestion that that does not change the meaning of the sentence but that it sounds [inaudible]? Can we adopt the text? Chris was suggesting "similar to the requirements under GDPR." Full stop. Not full stop, but "requirements under GDPR," without specifically referring to 61F.

Chris?

CHRIS LEWIS-EVANS: Thanks, Janis. No, 61F is well at the end. So it's just my shorthand. Sorry. Thanks.

JANIS KARKLINS: Okay. Then also Berry is suggesting that we can put in the brackets data that may otherwise be redacted to clarify what we're talking about. This points to Dan's question on implementation.

So can we live with this and replace those two points with [inaudible] geographic regions to this one bullet point?

Dan?

DAN HALLORAN: Hey, Janis. Thank you. I'm sorry. I don't mean to take up time. I know you're mostly focusing on this EEA versus non-EEA thing, but I'm still caught on: if the requested data contains personal registration data. The parenthetical is not helping me out. I'm just trying to put myself in an implementation point of view. If I'm, let's say, centralized requester or even a [inaudible] registrar or registry and I pull up a registration record and it says the e-mail is dan@ICANN.org, I'm not sure if that's personal data or not. Or, if it says CEO@ICANN.org, is that personal data or not? We had that debate a little bit, and I just don't know if there is any clear test that can be applied.

I think we've also pushed past it but I think I have a broader issue with the beginning of Bullet 6. It says, "The authorization provider may evaluate underlying data." I don't want to drag us into another may/must/should debate, but that's a little unclear, I think, from an implementation point of view. Is the team assuming that, in every single case … It's unclear to me, especially if you have a centralized provider, if that provider is always going to have to

grab the registration data and look at it. Then that brings me to that point which I think Sarah had raised earlier in the text of the building block, which is, how can a provider just look at a piece of WHOIS data and do this test and then do some of the tests that are required in Paragraph 7. Again, I think we're maybe building a lot into looking at a piece of registration data that I'm not sure you can do all that testing on. Thank you.

JANIS KARKLINS: I could argue that probably the response will be slower at the beginning, once we will start operations of SSAD. But, as we proceed, I think patterns will emerge and things will get clearer as we go.

Honestly, if you think that there is some linguistic fix that needs to be done in order to help ICANN org in implementation, whenever we will get there, please tell us what is your suggestion, what you think would help you in implementation, whether that is a centralized or decentralized system or a hybrid system.

Daniel, please?

DANIEL HALLORAN: Thank you, Janis. Sorry. I don't intend to slow this down at all. Maybe I can come back and consult with my colleagues and come back with something in writing. I just wanted to flag that I think there's a potential issue there with assuming. It should be really clear whether or not and in what cases what the authorization provider is going to do with that. That's going to be its own processing step. It sounds like, if it's a centralized model, it's its

own data transfer, just to get that data to the authorization provider to review the data. And you're going to need a legal basis for that step. So there's a lot in that. There's a few words that we're talking about, and it should be really clear under what circumstances and what's the basis and what's the testing the provider will provide. Thanks.

JANIS KARKLINS: We need to look holistically at the whole process, which we're trying to describe here, starting from the moment a request arrives and then what are the logical steps that the authorization provider should followed based on requirements of GDPR. We're trying to describe them one by one until we come to the point which suggests that, if a request does not contain a question about personal data, then it should not be further treated. If there is a request for personal data, then we need to do the balancing test, as required by GDPR or any other similar requirements [inaudible]. Then, in the next step, we describe how this balancing test should be done and what would be the response.

Ultimately, we are talking about the initial proposal, the initial report. Once we will get through the whole of building blocks, we will put it together and then we will do the final reading of the initial report before its release. Then we will probably find out redundancies and maybe (but probably not) inconsistencies. Then we would deal with those inconsistencies throughout the whole report.

Therefore, I would simply say we have spent now one hour only on this topic, and we have many other things to deal with. So my

question now is, is there anyone on the team who cannot live with this current proposal as described on the screen?

It seems that everyone [inaudible]. So then we will stabilize this text for the moment and then see what type of fix needs to be done once we will get to the final reading of the initial report. Thank you.

Can we go back now to the previous point and see whether the suggestion made by Laureen for implementation guidance is something we could accept? Laureen's proposal is, if the authorization provider does not approve the request based on another reasonable [inaudible], it [won't] achieve the same result. Then the authorization provider must identify the [inaudible] data to the requester. So can we accept this proposal as a part of implementation guidance of this building block?

Thomas?

THOMAS RICKERT: Thanks very much, Janis. I apologize upfront if I'm painful for you guys, but I have difficulties understanding what problem we're trying to resolve. Less intrusive may be that data is publicly available. But still, I think James made this earlier about the fee structure. If somebody is willing to accept a fee for getting data, then so be it. But I fail to understand why the authorization provider should be a depository of sources where data can be obtained. Those sources might be less legally sound as the one that we're creating. So I think, if we have a legal basis for disclosure, we have a process that ensure to the best possible

extent the rights of the data subjects. Making an organization where we create the authorization provider [that] points somebody to a source that is less accountable is troublesome to me. But may it only be me. If somebody can explain to me what problem we're trying to solve, I might be able to subscribe to it.

JANIS KARKLINS: Thank you, Thomas. One example that came out that I remember from the previous conversation last Thursday was that, if the contact e-mail is on the website, then you can have it there, not [to] the SSAD.

Let me take Alan Woods and then Milton.

ALAN WOODS: Thank you, Janis. This is going back. My hand was up many, many moons ago. So it happened to go on [inaudible]. With regards to Laureen's addition there, I do have conceptually a few issues with that, and that is, again, that there is a tendency here to flip the onus to that of the disclosing party here. That's not what we should be doing here. But you're basically saying this implementation guidance is that the disclosure should know of the more or less invasive means by which they can get this data. But, a disclosure: I'm a registry. If I was the discloser, I can't possibly know all the reasons for which data could be disclosed. That is up to the requester to say, "Hey, I have tried all these other areas. These I believe are reasonable, and I know not of any other way in which I can do that."

Now, if it is particular to that particular disclosure that they understand and they know there is a least intrusive way of doing that, they can point that out. But making that implementation guidance on this policy is pointless.

So that's my opening [gather] on that. I don't agree, definitely, with that implementation guidance. But I think what we really need to do here is check ourselves ever so slightly because, ultimately, whoever the disclosing body is is going to have to be the ones that legally stand up to scrutiny on this. To be perfectly honest, we should probably leave it as just the first bullet, and then the disclosing party, whoever that is, should be making these decisions based on their own legal advices in the particular case.

So, as then setting of a policy, we are going into far too much detail in setting that as a policy. That is not a policy. That is a legal call based on the way that the law must change peculiarly, again, as time goes by. As a good example of that, Theo Guerts from the registrars shared with a few people earlier today, not on this particular group, about how, in Romania, the concept that a debt-collection agency contacting a person through a phone number was actually a breach of data protection law because there was a postal address on file, and they should have only been able to use the postal address. Retaining the phone number in order to contact that person in order to call in a debt was considered an incompatible and unnecessary purpose.

So the law changes and the law will change and it really should be up to the disclosing party or the disclosing body to have the flexibility. We're not giving them that flexibility right now. We're setting it up to fail. So I just want caution against overly

prescriptive recommendations here because they're not going to help whoever that disclosing party is at the end of the day. Thank you.

JANIS KARKLINS: Thank you, Alan. Also, I remember that, in a different building blocks, we have a recommendation that, in the case of refusal, the authorization provider should provide an explanation on the reasons of the refusal. So that also needs to be taken into account.

Let me take Mark Sv and then Laureen.

MARK SVANCAREK: Thanks. Yeah, after all this discussion, I do think this bullet id redundant because "reasonable" and "less intrusive" is already part of the balancing test, so we don't need to call it out separately. And "must identify the less intrusive way" is already part of the justification of denial. So it does seem as if this bullet is redundant. It's more specific, but it doesn't really add any additional policy guidance. Thanks.

JANIS KARKLINS: Thank you. Mark, you're talking about Laureen's proposed implementation guidance or you're talking about the bullet itself? "consider whether reasonable and less intrusive means will achieve the same goal."

MARK SVACAREK: I'm talking about the bullet itself. Regardless of what language you put in there, we will have a consideration of proportionality in the balancing test, and we will have an obligation to explain why you denied something somewhere else in this guidance. So I don't think you need the bullet at all. Thanks.

JANIS KARKLINS: Yeah, but yeesterday some groups strongly favored retention.

MARK SVANCAREK: Yes, I understand that. But we have discussed it further today. Although I was okay with it before, now I'm increasingly thinking that – I think Alan said this – we're just becoming more and more specific but not really adding any additional guidance. Thanks.

JANIS KARKLINS: Thank you. Laureen?

LAUREEN KAPIN: I would certainly be comfortable with eliminating then entire thing, starting with the reference about "considering whether less intrusive means." I do agree with Mark in that I think it is redundant of the general balancing test.

But in response to the objections raised, my proposed language only relates to what I consider to be the narrow circumstance where the sole reason that the request is being rejected is because there's a less intrusive means. I would assume that the requester is going to make whatever showing it needs to make

that it has fulfilled their obligations. Certainly, if they're stating, "I've looked for the data. It's not publicly available. I've looked on the website. It's not there," etc., etc., and then it's rejected because there's some less intrusive means, I don't think it is an undue burden on the authorization provider then to identify that less intrusive means. This is a very narrow situation.

But, if we eliminate the whole thing, I'm fine with it. I'm also fine with putting this in the different section that talks about how, if the request is rejected, you have to provide the basis. But, if we're going to get this specific about this less intrusive means, then I think there should be an obligation to identify that less intrusive means.

JANIS KARKLINS: The proposal is now to delete both. After all these attempts and time spent in talking through this issue, can we live without this second bullet point, as you see now in the building block? Because we will retain the first bullet point, which is something that we all did yesterday. Yesterday, we agreed that "necessary" means more than "desirable" but less than "dispensable" or "absolutely necessary." So we would retain that, and the proposal is to delete the second bullet point [inaudible] after being better informed than last Thursday. Can we live with this proposal?

Okay. I see no objections, so then we take it out. We can move to the last unresolved issue in this building block, and that is Bullet Point 7. Specifically here the discussion was on what form we need to use in order to reply, whether "should," "may," "must," and so on.

After reading all the proposals and commentaries that have been provided, we came to the conclusion that maybe the right way forward be to use is, “The data is expected to be disposed,” rather than, “should, “must,” and so on. If all other requirements of disclosure have also been met, the data must be disclosed.

Also, I would like to remind you that there was a question to ICANN org on whether, in an implementation phase, one could enforce the term “should.” I don’t know whether there is already an answer ready from ICANN org on this.

But, before that, I would like to … Let me take Daniel first and then Mark Sv afterwards. Daniel, please go ahead.

DANIEL HALLORAN: Thank you, Janis. We’ve been consulting with colleagues and working on our written response to the team, which – I’m sorry – is not ready to share. But I can tell you in summary that it would be possible to enforce something like that, but it’s much cleaner from a compliance point of view to have a “must,” obviously, or to say that it must be disclosed, except under certain enumerated exceptions. If you say it should be disclosed, then you get in a fight with the registrar over whether the reason to not disclose was valid or not. ICANN Compliance might think the reason was not valid and the registrar – let’s say it’s a decentralized model – thinks the reason it has to dispose was valid. Then you have to fight it out or go to an arbitrator. So it’s messier but it is possible. Ultimately, there’s a reasonable test.

So that's just a summary. We can come back in more detail later, if that would be helpful, if this is still a live issue after this discussion. Thank you.

JANIS KARKLINS: Thank you. Mark Sv, please? I know you have an issue with it.

MARK SVACAREK: Yes. Yes, I do. The more I've thought about this and consulted people at Microsoft over the weekend – I'm sorry that I didn't declare this sooner – it really does need to be either "must" or "shall," for the reasons that Dan just listed. There's an enumerated list, and we can make the enumerated list as long as we want. I'm okay with having that discussion. But, at the end, it must be unambiguous. There has to be some of an expected outcome and clarity based on the "must" and the "shall," which is what's really required.

Also, as Dan said, you can go to arbitration. You can file injunctions. If you are being unlawfully compelled, there are ways to act outside of the policy. But the policy itself must be definitive, unambiguous, etc. To that end, it's either going to have to be "must" or "shall." Thank you.

JANIS KARKLINS: Okay. Now, when we're looking to the text on the screen, the proposal is to replace "is expected to" with "shall." Probably then the last sentence involves [inaudible] [deleted]. So that is the proposal.

Let me collect a few reactions before we proceed further. Alan Greenberg and then Alan Woods.

ALAN GREENBERG: Thank you. I put my hand up in relation to what was there until a minute ago. I was the one who raised the issue originally and said that it can't be "should" because that's not enforceable. "expected to be disclosed" I could accept, but I thought the proposal was that, if it is not disclosed, the rationale for not disclosing must be documented, whereas the next sentence we have here seems to be just the opposite, that you only have to document it if you disclose. So I'm a little bit confused as to how we ended up with the rationale for "approval should be documented," when I thought we were adding the rationale for "refusal should be documented."

JANIS KARKLINS: No, no. Here, Alan, we are talking about a situation where the authorization provider determines that the request of legitimate interest is not outweighed by the interest of fundamental rights and the data should or must, or now shall, as suggested by Mark Sv, be disclosed. And the rationale for approval should be documented. This is more for the logging purpose and documentation purpose for further auditing. So that is, I think, logical.

ALAN GREENBERG: Janis, to be clear, my original suggestion was to change it to "must" or "shall." The leadership proposal said "is expected to be." I'm happy if it says "shall." That goes back to addressing the

original problem I raised. If we're using "is expected" then the next sentence has to be the reverse of what it says. Or adding a new sentence saying the reason for refusal must be documented. Thank you.

JANIS KARKLINS: The rationale for denial or refusal also should be documented, and that [is] in the response requirements. So the baseline then is that every decision should be documented.

ALAN GREENBERG: I'm happy if it says "shall."

JANIS KARKLINS: Okay. Let me see if there is opposition to "shall" instead of "is expected to."

Alan Woods, please?

ALAN WOODS: Thank you, Janis. I'm going to be the person – I'm sorry – that says, no, I do have an objection to it. At the baseline to that objection is the fact that, really, we don't know who's making this decision yet. Really, there can be a distinct difference in the language based on who is the person footing the risk here, basically.

In this instance, if the Strawberry Team's responses come back from the Data Protection Board as supporting out of a centralized

model, then I think it's probably within the realm of possibility that this is a sort of recommendation that can be enforced because it's part and parcel within the one specific entity that is going to take on this entire mantle. Therefore, something like "shall," might very well work.

But, if they don't come back and it suggests a decentralized or hybrid-type model, what we're basically saying here is that we are giving the contracted parties, who'd be ultimately making this decision, absolutely not wiggle room in their interpretation and application of the law, again, noting that the law is not a set thing. It is a principle-based law that will change over time.

So what you're saying there is that we are going to ensure that we are going to enforce or we're going to make it a point that we're going to have to enforce that a person must disclose data in the way that we in 2019 or the early days of 2020 are going to tell you must do that. That is increasing the legal risk on the contracted parties in the hybrid.

Now, I understand and completely appreciate where Alan is coming from from the ICANN Compliance point of view, in the sense that you can bring that to arbitration, but, again, it puts contracted parties in that instance in a very, very difficult position because we're going to have to be arbitrating against our rights to enforce or, indeed, to apply the laws that apply to us individually. I think that will cause a larger, wider, broader issue when it comes to contractual enforcement, anyway.

So, again, I would caution us against that. Again, we're all at this table saying, where disclosure is deemed to be possible, we do

not need to be beaten into the corner with sticks in order to say you have to, in all particular instances, do this because you're punishing all of us for the few that maybe don't respond. I think that's where we should be focusing our "shalls" and our "musts," not on ensuring that we're all being with equally large iron bars in this one.

So, again, we are not creating something that is enforceable. We are creating conflict and we're creating an issue. I just want to warn us against that. If that means that we can leave it a bit more permissive and rely on having a spirit in this, I think we should go with that because it will help us move forward.

JANIS KARKLINS: Thank you, Alan. I thought we're working on the standard. If we are departing from that premise, then it doesn't matter whether the standard is applied by one or the standard is applied by 2,000+. A standard is a standard. So I'm just trying to understand what's the difference in your mind between application of the standard by a centralized decision maker or application of the same standard by 2,000+ registries/registrars following the same rules of the game. What's the difference? I simply do not understand it.

ALAN WOODS: If I can just jump in very quickly, Janis, and say, well, there's a very simple answer to that: one of us has one jurisdiction and the rest of us has 2,000+ jurisdictions. That's a very simple difference. There are many more in that. So the risk profile is completely different for both. So, again, we can't really make a decision on

whether something is permissive or mandatory unless we know what that actual jurisdiction is as well. That's why I'm [inaudible]. I think this is one of those we might to put a pin in and come back to once we have a discussion and a hopeful response from our European Data Protection Board friends.

JANIS KARKLINS: Okay. Let me take James and then Alan and then Mark Sv again. James, please go ahead.

JAMES BLADEL: Hey. Thanks. Mostly, I'm not going to disagree with anything Alan said. I just want to point out that – I think this goes back to the intervention from Dan and CIANN staff – if we're creating a policy that boxes in contracted parties and their ability to exercise any discretion.

I know that the temptation is we believe we're making something more enforceable from ICANN Compliance, but, really I believe we're significantly increasing the likelihood that we're creating conflicts with external legal obligations. In that case, we're just going to disregard this policy, and Compliance can pound our door and ring out phone all they want, but, as Dan said, it'll move to an external venue. I think that the concern that I have is then the entire policy looks like it's at risk because we're not creating sufficient pressure relief values, if you will, to prevent this thing from self-destructing.

But, if that's the direction that we're going, I just want to note that concern, that we are significantly amplifying the risk that this

whole thing could come tumbling down like a house of cards if we paint a box that is too narrow and we remove the ability for data controllers to have any discretion at all. Then the likelihood that this thing just evaporates in a puff of smoke goes up significantly. Thanks.

JANIS KARKLINS: Thank you, James. This is exactly I would like to certainly avoid at all costs. So that's why we're spending so much time in talking these things through and looking for solutions. So I would be last one who'd impose something that people cannot live with. If you cannot live with it, then it is not a solution.

I will take three more interventions, and then I will simply propose to park this last point and to note that in list of building blocks and move on to the next one. Mark Sv, Franck, and Margie, in that order.

MARK SVANCAREK: As Alan says, I hate to be that guy. I recognize his point that we will reexamine this once we know who the decider is – that's fine – but I can't agree to any language that doesn't provide some sort of certainty. As James says, if he's in a situation where he has to go to external arbitration, I think that's fine. We have a policy and that's going to be the policy. If the policy is forcing people to be compelled to act in unlawful ways, then they have recourse. But if the policy is, "Hey, you follow all the rules. You do this enumerated list and a whole bunch of other stuff, and I can still pull the rug out from underneath," I could never accept that. So I

just wanted to be really clear. I need some certainty here, or else I won't be able to [inaudible]. Thank you.

JANIS KARKLINS: Thank you, Mark. We are a team. This is what we're doing here. We're trying to find the solution that works for everyone. If you're [fighting the law], then probably we need to take a step back and revisit issues once we will have additional information.

Franck, followed by Margie.

FRANCK JOURNOUD: Thank you, Janis. Just for the record, to support what Mark has said, we need to have not certainty in the sense that I want to be certain that I will always get the data but rather certainty for the predictability that the policy states very clearly what every party has to do, the steps they have to go through, the reasons that should motivate their actions, etc.. To have a broad escape clause of "Unless you don't want to" isn't [inaudible] by saying, "Because of this, or "Because of that, because you [inaudible] that, that consideration renders the whole policy moot. So that's why we're, for IPC at least, concerned about that.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: One of the things that I think I wanted to point out is that the temp spec used the word "must." In our view, this is a step backwards if

it isn't a "must" or a "shall." To address the issues that James and Alan have raised, I think the instances that you're most worried about are the instances where the balancing test doesn't weight in favor of disclosure. So the elements that are listed in doing the balancing test I think give you that assurance that you have that ability to say no because it talks about legal framework. It talks about other things.

So, as Franck mentioned, we're living with that uncertainty into how that balancing test is going to be applied, but once the balancing test does weigh in favor of disclosure, then it should be "must" in the same that the temp spec says must. You can just simply take a look at all the enforcement action that has happened over the last year. ICANN isn't going to do that, and they haven't done it willy-nilly, related to disclosures under the temp spec.

So I don't think that the concern that ICANN Compliance is going to go after you for things we all think is reasonable is actually a valid concern.

JANIS KARKLINS: Two more and no more then because this conversation I think brings us more apart than together, specifically on this point. Alan Greenberg, please, followed by James.

ALAN GREENBERG: Thank you very much. I had my hand up earlier, but somehow it dropped. I get the feeling we're having the same discussion that we had last time we discussed this one. The rationale provided by some of the contracted parties was that they may have some

overriding reason to not disclose. This is someone who is proven they're slimy and abuses the system regularly. That's why, at that point – I, anyways – agreed to things like "expected," but you had to document why you were refusing so the clients could take action and decide whether you reason was justified or not.

So I'm happy with "must." I'm happy with "shall," and I'm happy with something somewhat weaker but is still enforceable. That's what it comes down to we have to make sure that bad actors are not refusing on a whim. Thank you.

JANIS KARKLINS: Thank you. James is the last one.

JAMES BLADEL: Thanks. I'm going to do something real weird here and change my mind and go ahead and agree with Margie and, I believe, with some of the other folks because, if I understand her intervention correctly, the point is that the release valve is not in the "must" and "shall" but the release valve is up above. If we can go back to the previous page, where the qualifiers are in the previous sentence: "If, based on consideration of above factors, the authorization provider determines," blah, blah, blah, blah, blah. Essentially, putting that in from of a "must" and a "shall" says, to me, if a registry or registrar is feeling at all queasy about a particular request, the discretion lives in this sentence and we can say we believe that this balancing test or consideration of the above factors do not provide the justification so that the "must" or "shall" clause is essentially not activated, if you will. If that's how we want

to interpret this – that the release valve or the discretion exits in the previous sentence in those qualifiers and doesn't exist in the second qualifier in the conditional – then okay. I guess I could live with that. I haven't checked with registrars, of course. They're probably screaming at me right now. But it feels like we just take – okay, the text just changed again … Okay, there we go. If we're going to put it ironclad in the conditional but the qualifier up above still maintains the discretion, then I guess we'll live with that part.

JANIS KARKLINS: Thank you, James. There are seven conditions that we agreed already on last Thursday that should be met. If they are met, then the personal registration data as requested shall be disclosed. If one of those conditions is not met or a few of them are not met, then of course this obligation does not stand. So that's the logic of things.

Also, another overriding premise is that the requester's legitimate interest is not outweighed by interest of fundamental rights of the data subject. So there are at least eight conditions with that.

So you can live with "shall." Let me see if there is anyone who cannot live with "shall." I know that Alan Greenberg can live with "shall." So let me ask, based on the conversation that we had, is there anyone who cannot live with the text which is now outlined on the screen?

James, that's your old hand or a new one?

Franck? A new one?

FRANCK JOURNOUD: I can certainly live with “shall.” I just want to point out that Alan Greenberg rightly suggests that the next sentence should read, “The rationale for approval for refusal” – not just “approval” – “should be documented.”

JANIS KARKLINS: That will be redundant because, if there is a refusal, then, in response requirements, the requester should be given reason for refusal.

On this specific point, in the next item, we have, “In case of refusal, the rationale for denial should be documented and should be communicated to the requester with caretaking to make sure that no personal data is revealed to the requester within this explanation.”

Alan, your hand is up.

ALAN GREENBERG: I’m confused with the text where that sentence has now gone, but wherever … all right. To restart this whole discussion in a different place, there should be “must” or “shall.”

JANIS KARKLINS: Sorry. I didn’t understand.

ALAN GREENBERG: The rationale for denial “must” or “shall,” not “should.” Again, there’s another “should” a few words later.

JANIS KARKLINS: Simply “must,” I think, because we have, in the building block, our response requirements that refusal is always with “must.”

ALAN GREENBERG: That’s fine with me.

JANIS KARKLINS: Staff will check [inaudible] uniformity in that. So can we close the discussion and approve this sentence in the building block?

Franck, your hand is still up.

FRANCK JOURNOUD: Sorry. Old hand.

JANIS KARKLINS: So it seems that we have stabilized this building block and it turns green, of course with the understanding that, once we will do the proofreading, the consistency reading, there might be a need to change a few things and make some tweaks. But, for the moment, I consider that the building block here is stabilized. Ah, so good. So, with this, thank you very much.

Let me go briefly, since we have only ten minutes remaining for the call, to the next agenda item, which is terms of use. As you

see on the screen, in this building block (terms of use), we have received very few comments. Those comments that have been received have been [inaudible] taken into account. There are only a few points that we have to discuss.

But my question is, are you in agreement that we do not the reading of every point that is on the screen? Because we have gone through the first reading. We have collected very few comments. Now there are a few outstanding issues that we need to address.

And if I may ask staff maybe to outline those three issues. Who would do that? Caitlin?

Caitlin, are you with us?

CAITLIN TUBERGEN: Sorry, Janis. I was having some muting and unmuting issues.

JANIS KARKLINS: Okay.

CAITLIN TUBERGEN: On the screen that Berry was showing, the two issues that were received before the deadline where Margie's question and Hadia's comment. So what Berry is highlighting shows, under privacy policy, the applicable lawful bases for each act of processing. Margie notes, "What is intended here, that any possible legal bases be listed?"

I see Margie's hand is raised. Maybe she can explain what she was asking.

JANIS KARKLINS: Okay. Margie, please?

MARGIE MILAM: As we were looking at this, we were really confused as to what the intent of the privacy policy was. We agreed with some of the comments that Volker and others mentioned, that most of this stuff, if you're talking about use of the data by the requester, is all covered by the disclosure agreements and not something that would go in a privacy policy.

So, when you think about what a privacy policy is, it's typically the rules that apply to the data that is collected by the service. So I think that's the requester data, but, again, it's very vague. If you're talking about the requester data, not the actual use of the data that you get from the disclosure process, because that's covered by a disclosure agreement with all the terms that we would have from our other building block, we have to be really mindful of what we're actually talking about in the privacy policy.

So, in that context, what legal basis are you referring to? Is it performance of contract? I just don't know what we really are intending here. So that was my question.

The only thing that I could see that isn't something that would be covered by the disclosure agreement with the requester is the thing that Hadia mentioned about how does a data subject get

access the data and perhaps correct it if need be and exercise its rights under GDPR. That's the only other thing that I thought maybe wasn't covered by a disclosure agreement.

So, as you look at this, you think about [inaudible] context. It's the data that the site – in this case, it's the SSAD – obtains from the requester or whoever else uses the system. So, in my view, that's not the same as the legal bases that we've been talking about before for what we actually do with the data that gets disclosed because that would be in a disclosure agreement subject to all the other terms that we've been talking about.

JANIS KARKLINS: Thank you. Marc Anderson?

MARC ANDERSON: Thanks, Janis. I have similar concerns as Margie does. I think maybe what can be done in the interim between now and when we pick this text up again is maybe staff can take an attempt at describing what the privacy policy is intended to cover, what the terms of use are intended to cover, what the disclosure agreement is intended to cover. Right now, they're just out there in the document and there's not really context that goes with them. I think maybe if we had some context around that, it would help. But generally I think I have the same concerns as Margie on this one.

JANIS KARKLINS: Thank you. First of all, this is not the first time we're talking about these things. On terms of use and lowering them in the text, I think

we have already disagreement on. But we have agreement on what the terms of use should contain. [The identification] of the disclosing party in ICANN data requester requirements, [inaudible] requirements, ability to demonstrate compliance, applicable [inaudible] on the disclosure agreement. We also have some agreement that, at the minimum, disclosure agreements should [address] use of data for the purpose indicated in the request. Requirements of use of data for a new purpose other than one indicated in the first. Retention of data, loss of use of data. So these are agreements that we have from the previous conversations.

On the privacy policy, this is a compilation of different proposals that have been put forward. I recall that, in one of the conversations, there was a rather simple proposal saying that the EPDP recommends that the entity disclosing data should develop a privacy policy. Full stop. And then nothing else on that.

Again, we can go different ways to address this issue. We can be very simple and straightforward. We can be more elaborate, but then [we need to] maybe spend much more time than we have on our hands.

I am very open. Maybe, since we are three minutes before the end of the call, what I would suggest is we're meeting now again on Thursday, two days from now. Please have again a closer look to this building block and the automation building block, as well to one that Caitlin will now recommend, which is next on our list. We will attempt to address these two outstanding blocks of use [inaudible] policy on disclosure agreement and on privacy, as well

as automation, as well as one other one, which will be? Caitlin, could you announce it? The next on our list.

CAITLIN TUBERGEN: Sorry, Janis. I am looking it up. One moment.

JANIS KARKLINS: Yeah. And we will take these three building blocks [inaudible] Thursday. I would also like to indicate that I'm traveling on Thursday and I will be able to chair the first part of the meeting, but then Rafik will take over after one hour, and I will rush to the gate. I will take the call from the airport. Response requirements will be the third item for the next meeting. If there will be [inaudible] and I will not be able to chair Thursday's meeting, then Rafik will be on standby. Otherwise, I will be on the first hour with the team, and Rafik will continue until the end of the meeting.

With this, I thank you very much. I think we did a great effort in finalizing an important building block. We will take three others on the next call. [Kavouss], thank you very much. I say that this meeting is over. Thank you, and have a good rest of the day. Bye.

[END OF TRANSCRIPTION]