ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Tuesday, 26 May 2020 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/qoYEC
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, good evening, and welcome to the GNSO EPDP phase two team call taking place on the 26th of May 2020 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 Matthew Crossman of the RySG, and Amr Elsadr, NCSG. They have formally assigned Beth Bacon and as their alternates for this meeting and any remaining days of absence. All members and alternates will be promoted to panelists for today's meeting. Members and alternates replacing members, when using chat, please select all panelists and attendees in order for everyone to see the chat. Attendees will not have chat access, only view access to the chat.

Alternates not replacing a member are required to rename their lines by adding three Zs to the beginning of their name, and at the

end in parentheses, their affiliation, dash, “alternate,” which means they are 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 the chat apart from private chats or use any other Zoom room functionality such as raising hand, 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 anyone has any updates to share, please raise your hand or speak up now.

Seeing or hearing no one, if you do need assistance with your statements of interest, please e-mail the GNSO secretariat.

JANIS KARKLINS: It seems we lost Terri.

TERRI AGNEW: Pardon. I did just get a notice that my line dropped, so I'm continuing on. Thank you. All documentation and information can be found on the EPDP Wiki space.

Please remember to state your name before speaking. Recordings will be posted on the public Wiki space shortly after the end of the call. As a reminder, those who take part in ICANN multi-stakeholder process are to comply with the expected standards of behavior.

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

JANIS KARKLINS: Thank you, Terri. Hello, everyone. Welcome to the 60th meeting of the EPDP team. We will start with the usual question, whether the agenda that has been circulated to the mailing list last Friday is acceptable for today's work.

In absence of objections, I take that the agenda is approved and we can follow, hoping that we would exhaust it by the end of the two hours' work. If not, then we will continue on Thursday. And actually, you received today also a notification that we may need to meet also on Tuesday in order to examine priority two comments or comments to addendum to initial report. And so in parallel, of course, there'll be work on the overall revised recommendations. But seems that we will need to have that meeting as well.

On housekeeping issues, I have only one thing to say. You were on copy. As a result of discussion during the last meeting, I sent e-mail with the questions related to ICANN Org possible involvement in operations of SSAD and with the request, if possible, to send replies by end of this week, and certainly as soon as I get replies, I will share them with you on the mailing list.

And in absence of questions at this time, I would propose that we move to agenda item four, which is continuation of examination of recommendation 13 on the terms of use.

We already examined two first topics during the previous meeting and we should take now up topic question number three. Caitlin, if you would like to introduce the question.

CAITLIN TUBERGEN: Thank you, Janis. With respect to question three, this deals with the privacy policy section of recommendation 13, and there was a suggestion that the privacy policy, the word following that should be "should" instead of "shall." And there wasn't agreement on that, so we'd like to pose that question to the EPDP team.

JANIS KARKLINS: Okay. Thank you. So it's not the first time when we are risking to spend hour talking whether it should be "shall" or "should." So just a reminder from the previous conversations, my understanding was that if there is "should," it is not enforceable, not compulsory. "Shall" or "must," it will be done [inaudible].

So, any comments or guidance whether we will change the initial recommendation but suggest that these eight elements shall be included in the privacy policy? And you see those elements on the left side of the screen.

Marc Anderson, please.

MARC ANDERSON: So I'm wondering if we could hear from somebody that's opposed to "should." My recollection of our recent conversations is that we generally seem to want flexibility in the drafting of the privacy

policy, and what's more, working group members have seemed to advocate for having that be a somewhat open process with the ability to comment and provide input on the creation of that privacy policy.

So I'm thinking that “should” is more flexible than “shall,” and “should” seems to better reflect what the working group has been discussing lately. But if anybody has arguments on why it should be a “shall,” I think now would be a good time to raise them.

JANIS KARKLINS: Thank you, Marc. Though I understand that if we’re using “shall” or “must,” that does not prevent other elements being included if that is about kind of listing items. I have a few hands up. Laureen and Margie.

LAUREEN KAPIN: Thank you. I'm wondering if we should try and agree upon a minimum set of standards here and create a floor rather than a ceiling. And I hear Marc’s desire for flexibility, and I think that is important, because indeed, there may be certain contracted parties that wish to go beyond a certain floor, and that should be encouraged.

At the same time, I do think we need some minimum standards that we would preface with the word “shall” because as we've already discussed ad nauseum, dare I say, if it’s a “should,” it’s not enforceable, which means it has very limited utility.

JANIS KARKLINS: Thank you. And also, you see that we are setting the minimum standard, because in the first sentence, we're talking about, at the minimum, which means that there may be also other elements included in that privacy policy.

LAUREEN KAPIN: Correct, Janis, but if you have minimum combined with a "should," it's unenforceable, period. That's the problem with it. So I very well see that "at a minimum" is there, but if you combine it with a "should," you may as well wipe the whole thing out.

JANIS KARKLINS: Thank you. That's not my intention, by the way. Margie, please.

MARGIE MILAM: Hi. Yes, I agree with Laureen. And I think, to address Marc's concern, in my view, they should be a requirement that's enforceable by ICANN. But as you can see, it doesn't specify exactly what each party needs to stay. So the flexibility is in how it's interpreted by the contracted party. So that's, I think, built into the policy the way it's written. But we need to keep the word "shall" or "must" in order to ensure that it is a minimum that ICANN Compliance can enforce. So as long as there's the ability of a contracted party to decide how that language reads as it relates to their customers, but that they've clicked off every single one of these and that's something that ICANN Compliance will look at as part of the audit, then I think it probably addresses Marc's concern. So I'm advocating for making it "shall" or "must."

JANIS KARKLINS: Thank you. Marc, are you convinced?

MARC ANDERSON: Thanks, Janis. I think I have to clarify something. First, I don't really feel strongly over "shall" or "should," I was just sort of raising my hand to reflect what we talked about earlier. But I have to respond to Margie and Laureen and just sort of remind you guys, this is the privacy policy for SSAD users. You both made interventions that make me think that we're not talking about the same thing.

This is the privacy policy that the ICANN—you both talked about forcing contracted parties to do something here, and this is about the privacy policy that would apply to SSAD users and how the SSAD system would use the personal data of requestors, SSAD users. So just to make sure we're talking about the same thing. It sounds like we're not. So let me just clarify or remind everybody, this is the privacy policy for SSAD users, not something that we're talking about applying to contracted parties or that ICANN needs to enforce on contracted parties. I hope that helps clarify where we are .

JANIS KARKLINS: Yes. Thank you. But the same applies to broader kind of set of issues. If you have "shall" or "must," that provides clarity and cannot be disputed. When you have "should" or "could," then that provides ambiguity. And sometimes ambiguity is good, sometimes it is not. Here, we're talking about kind of a minimum standard that

what elements SSAD users should adhere to, and I think that that is minimum that must be in those, and then maybe something else.

But again, I'm not arguing on either side. We agreed in an initial report to put “shall.” It has been contested during the comment periods or commented during periods. We’re repeating the same conversation, and probably on item seven, we will repeat it again.

Alan Greenberg, please.

ALAN GREENBERG: Thank you very much. I put my hand up to say I'm confused, but I'm more confused now. When we say this is the policy for SSAD users, which I presume to be requestors, is this the policy that they must adhere to with the information, or the policy the SSAD will apply to their information? I thought it was the policy the SSAD should apply to the information provided by users. And I can't see how it can't be a “shall,” because we’re not going to be compliant with GDPR and other privacy legislation unless we do have those kinds of statements to tell people how we’re going to use their data.

Now, if we’re talking about it’s the rules that the requestors must use and how they treat the data, I thought those were the commitments they make in using the data. That’s not a privacy policy, that’s a commitment. So I'm getting very confused about exactly what this policy is governing and who it is that’s going to write the policy. I thought it was a policy for the SSAD talking

about how we treat requestors' data. If it's not, can we be more clear, please?

JANIS KARKLINS: Thank you, Alan. Franck.

FRANCK JOURNOUD: Thanks, Janis. I think I'd make a point similar to what Alan just said, that when you look at those bullets, those are kind of chapters of a privacy policy. We have no details—and I'm not saying we should have details. We have no details under them. I can't imagine, I've never seen a privacy policy—at least one that would be complaint with any privacy law—that would not include these things. The type of personal data processed, that's like the first line of a privacy policy. We process this kind of data for this kind of purpose, this kind of way, subject to this kind of consent, etc.

So if anyone's privacy policy is missing any of these items, then I don't see how it's compliant with any privacy law. There might be one or two, but no, I'm reading this and it's like, all of this has to be in there.

JANIS KARKLINS: Okay. First of all, I think that this is the privacy policy that will govern the treat of data by users and in general in the whole SSAD. So if that needs to be clarified, staff can make this attempt to clarify. That said, I felt that Marc was not adamantly opposing to maintain "shall" and all others spoke in favor of retaining the

formulation of our initial report, and I would suggest that we do not change this determination, “shall,” and move on. Any objections? Thank you. The next question, Caitlin, please.

CAITLIN TUBERGEN: Thank you, Janis. Question four was a public comment that we received that is requesting to add three additional bullets to the list, and those bullets are transparency requirements, data security requirements, and accountability measures. And we needed to check if the team is in agreement with that addition.

JANIS KARKLINS: Thank you. Very clear. Is there anyone who would speak against adding those three bullet points to those eight that are already there? No hands up, which means that no one is objecting. So staff will add them for the final reading. Please, Caitlin, number five.

CAITLIN TUBERGEN: Thank you, Janis. For number five, we’re dealing with the first bullet under the list, the relevant data protection principles for example, and a commenter noted that this sentence appears to abruptly cut off. And asking if that is the design of the EPDP team or if sub-bullets were inadvertently cut off, and if so, what those should be, or if instead, the “for example” should be stricken.

JANIS KARKLINS: Thank you. That's a very pertinent observation. So it means that somebody has read those initial recommendations and spotted our mistake, basically. So, what is the prevailing feeling among the team members? Shall we attempt to put some bullet points, sub-bullet points, or we just keep it very short, relevant data protection principles and let implementation or drafters of this privacy policy to deal with that during the implementation phase? So I have Milton who says "strike" for example. Matt Serlin supports, but then I also have four hands up. Mark SV, Brian, Georgios and Alan Greenberg, in that order.

MARK SVANCAREK: Thanks. It looks to me like that bullet really belongs in the first sentence. The EPDP recommends at a minimum the privacy policy shall include relevant data protection principles. For example, bullet, bullet, bullet. All the bullets are relevant data protection principles, or maybe specifics. But you could either strike it or you could move the text of the bullet up into the main body. So either of those would be fine with me. Thanks.

JANIS KARKLINS: Okay. Thank you. Brian, please.

BRIAN KING: Thanks, Janis. I raised my hand to say the same thing as Mark. Thanks.

JANIS KARKLINS: Okay, so the proposal is to delete “relevant data protection principles, for example,” but formulate the first sentence of this section, “EPDP recommends at a minimum the privacy policy shall include relevant data protection principles.” And then the colon.

If there are no objections, staff will correct that. Thank you. Number six.

CAITLIN TUBERGEN: Thank you, Janis. Question six deals with the sentence that Berry has highlighted on the screen, and there was a public comment asking if that can be removed. And if it can't be removed, can the team be a little bit more clear about which recommendations it is referring to here that are specific to the terms of use or if there's just a blanket recommendation.

JANIS KARKLINS: Okay. Thank you very much, Caitlin. So Brian, please.

BRIAN KING: Thanks, Janis. I think now that we’re less confused, I think this concept might need to be somewhere else, and it’s probably already captured somewhere else. In my view, this is knowing the RAA and what it requires contracted parties and registrars specifically to notify registrants about, I think that lacks the specificity that GDPR requires, and this might be trying to address that. But now that we’re clear that this is talking about the terms of use for the SSAD, I think this language is probably still needed, although not here. Probably in the part where we talk about how

the contracted parties need to tell the data subjects about when their data is collected. I hope that's helpful.

JANIS KARKLINS: Okay. Thank you, Brian. So I have Alan's hand up. Alan G.

ALAN GREENBERG: Thank you. My comment was going to be somewhat similar, but a little bit more general. I don't think it applies here at all, but surely, this is a global statement about our overall work that when we're finished, there's almost no doubt in my mind that this policy will be amending the RAA, and someone should be going over the RAA with a fine tooth comb saying, are there any other things we need to put in to make sure this policy is going to be implemented — the EPDP policy overall would be implemented and implementable. But it certainly doesn't apply here.

JANIS KARKLINS: Okay, so then the proposal is to remove this sentence from this recommendation and add kind of a general observation in the preamble to recommendations that after adoption of recommendations, the registry agreements should be updated accordingly or when necessary, something like that. Alan, are you in agreement?

ALAN WOODS: I'm not going to answer that question.

ALAN GREENBERG: Yeah—sorry, I don't know which Alan.

JANIS KARKLINS: Alan Woods.

ALAN GREENBERG: If you're asking me, it's both this RAA, and of course, the registry agreement. Both of them, this policy is going to be amending both of those as a matter of just what it's doing. So we may want to state that somewhere. Thank you.

JANIS KARKLINS: Okay. Thank you, Alan G. Alan Woods, please.

ALAN WOODS: Thank you. All I'll say to that is we're creating a consensus policy here which is what—it is incorporated into the agreements by reference. We're straying into that territory we all don't like at this particular point in time. So throwing around things like "we probably will have to amend the RAA and the RA and this," no, let's create the consensus policy and then see what the GNSO and the community and the different stakeholder groups need to do then with that. But this is a consensus policy, it is by its very nature changing the contract.

JANIS KARKLINS: Okay. Thank you. But you're not opposing to delete it in this particular place, I understand?

ALAN WOODS: No. Again, I do find that a lot of these things are unnecessary because we're going into too much detail, but yeah.

JANIS KARKLINS: Okay. Thank you. Becky.

BECKY BURR: I just wanted to echo, I'm very wary of using the word "amend" because I don't think—obviously, consensus policy creates obligations that can be enforced through the contract on contracted parties, but I don't think amending is the right word. It would require modification to the contract, but I don't think that in this particular case, the use of the word "amend" is the right one.

JANIS KARKLINS: Okay. Thank you. Beth, please.

BETH BACON: Thanks very much. I also will plus one to Alan and Becky on their comments. I do want to just clarify, I think that we should keep in mind with this where it says further consideration should be given during the implementation, that doesn't mean the IRT is going to draft amendments and changes to their RA and the RAA. Implementation means that, as Alan said and as we're putting in effect for phase one, the GNSO may find that there are things that are conflicting and then the RA and RAA may need to be amended. However, that needs to be triggered by the contracted

parties and we would do that to ensure that everything is correct. But as Alan says, if the consensus policy becomes part of the contract, then those changes are essentially made. but I do want to be clear that we might want to rephrase implementation simply so there's no confusion with the IRT, because that's not the task of the IRT. Thanks.

JANIS KARKLINS: Thank you, Beth. No, for the moment, proposal is to delete this sentence which is marked in blue, and question is whether to put something somewhere else or not. And seems to me that prevailing opinion is that if that is consensus policy, it will be applied anyway. Or rather, when it becomes a consensus policy, it will be applied. Marc, your last word.

MARC ANDERSON: Thanks, Janis. I agree, I support deleting it. It clearly doesn't apply in this section. I think it was Brian who had concerns about applications on disclosing to data subjects, how the data would be used. I just wanted to point out that that's already covered in other sections, specifically recommendation 11, disclosure requirements, Section H has the obligation to provide concise, transparent, intelligible ... notice to data subjects how their data will be processed. So I think this concern is already addressed [inaudible] clearly, this doesn't apply here and it can be deleted from the section.

JANIS KARKLINS: Okay. Thank you. Then I would suggest, based on this conversation, that we simply delete this sentence and move to the next item, which is number 7. Caitlin.

CAITLIN TUBERGEN: Thank you, Janis. We might be able to skip question number seven since it's identical to number three regarding the use of shall and should, unless anyone has an objection to keeping the word "shall" as it is in the [inaudible] recommendation.

JANIS KARKLINS: Let me see. Can we maintain the initial recommendation as is by "shall" based on our previous conversation 15 minutes ago? No objection? Number eight.

CAITLIN TUBERGEN: Thank you, Janis. For question number eight, it deals with the first bullet and the terms of use section, which addresses indemnification of the controllers, and commenter is asking the EPDP team to clarify which party is responsible to indemnify whom, and also who is being referenced as the controller in this section.

JANIS KARKLINS: Thank you very much. Any comments? Probably controller is the one who makes the disclosure decision, and since we have working hypothesis that we have joint controllership, then decision

is made either by the contracted parties or by the central gateway. Brian.

BRIAN KING: Hey Janis, thanks. I won't touch the controllership thing, but to the part of the question I can answer, it was my understanding that the requestor would be the one indemnifying here. So if that helps to change the passive voice there, we could say “requestors’ indemnification ...” and go from there. Thanks.

JANIS KARKLINS: Okay. Thank you. So, is that common understanding? Seems to me. So I then ask staff if there is a better formulation as suggested by Brian, please apply it. And in absence of further requests for the floor, number nine. Caitlin, please.

CAITLIN TUBERGEN: Thank you, Janis. I believe this was a question from the ICANN Org liaisons noting that these bullets seem to be a mix of liability considerations and rules, and asking if this was the intention of the team.

JANIS KARKLINS: My initial comment would be if that is in the policy or draft policy, that was intention. But I'm not overly sure that I understand the concern here. Maybe ICANN staff liaison could explain the concern here and what is the consequence or why you're asking this question.

DANIEL HALLORAN: I'm sorry, [I confirmed with Eleeza,] actually, I'm not sure what this is referring to either. It looks true that the section says the terms of use shall address, and then the first bullet is indemnification and the remainder seems to be restrictions on the requestor, but I don't see the problem with it at this minute. If it's from us, you can withdraw it, I guess.

JANIS KARKLINS: Okay. Thank you. So then we will skip this and move to item 10.

CAITLIN TUBERGEN: Thank you, Janis. Last but not least, that last set of bullets in the recommendation, the commenter is asking if they're supposed to be requirements for contracted parties or requestors. And If that could be clarified.

JANIS KARKLINS: Thank you. Marc Anderson, please.

MARC ANDERSON: Hey Janis. My recollection on this is that the disclosure agreement is intended to be drafted by the disclosing entity and apply to the person requesting the data. So the disclosing entity—let's just say hypothetically a registrar is the disclosing entity for the request—then they would have a disclosure agreement with the entity requesting the data, and that disclosure agreement shall address

each of these four bullet points. So I hope that clarifies and I'm not completely off the wall here.

JANIS KARKLINS: Thank you. You're not, because that is the overall terms of use of SSAD, and this is a part of it. Margie.

MARGIE MILAM: Hi. I actually don't think it is with the contracted parties, because that would mean that a requestor would have to have thousands of agreements. I think it's with the SSAD as it relates to the disclosures that take place throughout the system. But I think it's one standard agreement that a requestor would sign in order to submit requests through the SSAD, and it would apply to all contracted parties. At least that's how it makes sense to me.

JANIS KARKLINS: Thank you, Margie. This is what I was trying to say, that this is the part of the overall terms of use of SSAD and that would be one part of it. Volker.

VOLKER GREIMANN: Yes. I'm of two minds on that. ultimately, I agree that the agreement should be with the SSAD and that's probably also the reason why I would say that the contracted parties will have to be at the table when the original agreements are being drafted, since at this time, when we're still providing WHOIS, we have this agreement attached to every WHOIS output and the requestor

basically has to agree to the terms of each contracted party in the disclosure of the data, the output of the WHOIS [inaudible] such as no repackaging and no redistribution and what have you.

So I think it's not beneficial for either the requestors or the contracted parties to carry on this practice of having individual agreements for each [request or with each request to the] contracted parties. That would become quite unmanageable. But I certainly think that we should be at the table when these agreements are being drafted so our requirements for such agreements are being met. Thank you.

JANIS KARKLINS: Thank you. I think we have clarified this. There is no contradiction and this is part of the overall terms of use of SSAD and will be applied as a blanket requirement to all requests after disclosure.

So I see no hands up, so we're on the same page. Thank you. That leads us to the end of examination of outstanding issues on recommendation 13. It'll be marked green on the website as examined. Of course, with understanding that it will be once again looked at during the final final reading using method of "cannot live with."

So now we're moving to recommendation 17, which is logging. And if I may ask Marika to kickstart the conversation and introduce the first question.

MARIKA KONINGS: Thanks, Janis. For this one, we've done the same as for the other recommendations, we'd looked at the input provided by the different groups on the discussion table, and from there, derived a number of assumptions or takeaways for those items where the groups that provided input agreed on the approach to be taken, and then we identified as well a number of questions where there was either disagreement or not sufficient clarity on how the group wanted to proceed. So in relation to that assumptions and takeaways for logging, there was one addition that was proposed and everyone agreed with, that commented in relation to the logs being available to allow requestors and contracted parties to review their own statistics as long as these logs do not contain any personal data. There was also support for clarifying and ensuring that the retention period must be sufficiently long, at least at first, to accommodate all parties' adoption to the system and to support evolution efforts of SSAD.

There was a comment that focused on privacy by design and by default. We noted there that it didn't seem to really fit with the logging recommendation as obviously the logging is the result of what is collected in the first place. So that is probably a consideration that the group needs to consider, or hopefully has considered as well in the overall design and recommendation relating to SSAD.

There were a couple of comments that expressed concerns in relation to disclosure decisions, but we noted that those should be or have hopefully already been addressed in recommendation six, contracted party authorization, as this recommendation deals with logging.

There was agreement that care must be taken to ensure that personal information has been removed from information that is logged, and if there is any information that is logged that contains personal information, there need to be appropriate safeguards and protections in place.

There was also agreement to add an additional E2, that contracted parties should be able to access these logs upon request as well as in order to verify their own reliance on the SSAD mechanisms. And there were a couple of comments that related to automation that we noted have been addressed or discussed in the context of recommendation 7 and number 16.

Based on that, we still do have a couple of open questions for the group. There were some questions around what details should be logged by the central gateway and manager in relation to disclosure decisions. There were suggestions here that the bullets listed here should be the information that should be logged. We would want to point out here that in the context of reporting requirements, there is already a proposal on the table that specific data needs to be reported upon and to report on that data, the data obviously needs to be collected, and this seems to largely align with the bullets that have been listed there.

There's of course a question, if the group agrees that it's okay to include this, is there any other information that should be logged in relation to disclosure decisions, and there was also a question raised whether the logging information should be proactively reviewed by ICANN Compliance to identify potential compliance issues. So that's question one.

JANIS KARKLINS: Thank you, Marika, for introducing question one. Alan Woods, please.

ALAN WOODS: Thank you very much. Two things. First thing is just with regards to the retention period we're talking of. I think we just need to be careful as well that we don't just leave it hanging out there that we say retention period must be as long as is necessary for us to figure out what we need to do with it. That's not going to pass muster, so we need to be careful on that. We should set a task that the retention period, once all is said and done, be that IRT or whatever, that it needs to be set in a concrete and transparent way for the data subject to know how long we are going to retain that data for that initial purpose. So again, that needs to be very clear. That was just an aside.

Going to question one, I think we need to be, again, exceptionally careful when answering the questions of what are in those logs. Number one, I do think that we're, again, creating this situation where we're absolutely duplicating efforts of what the law will require. Any disclosing party doesn't maintain a log of why and how and when and for what reasons they disclose data, it would be silly of them. they would not be able to show transparency and compliance, not just be compliant.

If we're saying that the log has to be kept centrally, then we're going to have a huge issue because that's an awful lot of additional personal data regarding that actual disclosure decision

that will have to be logged somewhere other than the disclosing party. So again, you're putting an awful lot of liability on whoever is holding that at that particular time. We're adding more layers of complexity to that.

If the question is a decision has been incorrectly made in the opinion of somebody who feels aggrieved, then the logs should be capable of being reviewed. And from a procedural element, ICANN then can say, "Did you maintain a log? Are you happy?" And in certain circumstances, there might be need, but it's not going to be norm for ICANN Compliance to see the actual decision making process. They're just going to be asking whether or not time and effort were into that.

Again, we're talking about the procedural versus the legal decision here. So again, we have to be very careful as to what additional responsibilities, liabilities, data transfers, accessing, and of course, processing we're taking just for the simple thing of creating a log which should already exist at the disclosing party. So we're making this a lot harder on ourselves. I think we're duplicating what the law expects. But I know I'm sure that we'll get the same chorus of, "But ICANN Compliance should be able to enforce this." I just really think that we need to set realistic expectations of what we can achieve, unless we want to add another $8 million to the annual review of this.

So there are my thoughts on that.

JANIS KARKLINS: Thank you, Alan. Mark SV, please.

MARK SVANCAREK: Thanks. I think it's sufficient to say the centralized logs shall contain no personal data. That's a privacy by design consideration. So if you maintain an index into the requestors, then you don't need to know what their personal data is. You know Microsoft is number 999, then all you have to do is log, "I got a request from 999, here is the result."

If it was related to a specific domain name, all you need to do is remember what the domain name was, or even, honestly, if there was a ticketing system, all you need to know is what was the ticket number, and then you can work backwards from that. But I think Alan was concerned that the centralized thing would have a lot of overhead because we'd have to manage all the personal data that might be going into it. I think we can just specify that there won't be any personal data that is logged into the central gateway, and that if personal data is needed for an audit, which I think should be seldom, you could go back to the controller and get that. Thanks.

JANIS KARKLINS: Thank you, Mark. Volker, please.

VOLKER GREIMANN: Yes. I would appreciate Mark's comment. However, sadly, privacy by design doesn't work quite like that, since even if you use an index number, that can be considered private data if it is possible to use that index number to figure out who the requestor was. If that then contains private data, we're back at private data. So we have to make sure that if we use an index number, it cannot be

traced back. Maybe a hash that isn't tracing back to any specific requestor. Maybe it's something different. Maybe we have a legal obligation to keep that data to make sure that we can audit the requestor at a certain point, but then we have to delete it. We just have to make sure the privacy by design is incorporated, and the index number alone will not fix that. Thank you.

JANIS KARKLINS: Thank you, Volker. Mark SV.

MARK SVANCAREK: Actually, what you described is privacy by design. A hash is just going to be an index number if it's a one to one match. Privacy by design means that the two tables that you don't want to be joined are kept segregated somehow, either they have different access controls or they're kept in different places. So depending on how the request is generated, the requestor identity would be kept somewhere different from the requestor reference number, which is in the ticketing system. That's by design.

So that way, the piece that is available to the controller might not contain any personal data at all. The piece that is logged by the gateway is separate from the mapping of the personal data to the index number. That's privacy by design.

So that segregation and prevention of easy joining is the privacy by design concept, and it does make the whole system more secure and private. Thanks.

JANIS KARKLINS: Thank you. Can we look really closer to the question as such, not speak in theory? So I think it is related to the implementation guidance [inaudible] recommendation 17. Berry, if you could scroll down, there is a bullet, logging related to central gateway manager, and probably there, the question is whether, to existing two sub-bullets, we can add also a proposed three. Beth, please.

BETH BACON: Thanks, Janis. I know you don't want to ask larger questions, we want to focus on this question, but I'm going to break your rule. I apologize. So as we look at the question being asked, what specific details are logged, and then also just the overall description of the purpose of the logging, I'm not sure what the purpose of this logging is for. Who is going to be doing the auditing? Is it of the SSAD decisions? Is it ICANN? Is it a DPA? Is it contracted parties? I'm very unclear as to who is going to be doing the auditing, what the auditing is for, and it would depend upon what party is auditing and for what purpose. It creates a lens through which we would view any of these questions.

So I apologize if I'm the only one that's a little lost on these details, but if someone could provide that clarity, that would be really helpful, because I think that really speaks to how we read these particular recommendations and questions. Thanks a bunch.

JANIS KARKLINS: Okay. Thank you, Beth. Actually, the auditing recommendation is next that we will be reviewing, and there are some issues, but it is mostly ICANN Org who will organize the auditing, if I may put it in

a very simple way. And logging information as consensus suggests would be information that auditors would look at first in case either to look how system works in general or if there is a very specific issues related or identified as systemic abuse or something that they would help auditors to review the allegations.

So I have two further hands up. Marc Anderson and Alan Greenberg.

MARC ANDERSON: Thanks, Janis. Beth made a really good point there. I was looking at question number one. I was having trouble understanding it in the context of logging, because it doesn't really seem to fit here. I'm actually wondering, I don't know who submitted this particular question. But I'm wondering if this is actually what this particular question is getting at is actually more of a question relating to reporting. Because I don't think that this information—I'm not sure that this question is really getting at an obligation for logging, I think it doesn't make sense for logging by itself or even really for auditing. I think maybe this is applicable to a discussion about reporting, which I think we have later on. So maybe this is something we should table [inaudible] conversation.

JANIS KARKLINS: Okay. Alan G, please.

ALAN GREENBERG: Thank you. I'd put up my hand in response to Beth. I wasn't even sure what the reference to auditing was. One keeps logs to be

able to understand what was happening, to look at performance, to look at overall volumes, and to respond to queries that may come in.

I don't think it's an auditing issue at all. I just didn't understand the reference to auditing.

JANIS KARKLINS: Beth, your hand appeared and disappeared.

BETH BACON: Sorry. It was an accident.

JANIS KARKLINS: Okay, but would you clarify the meaning of your intervention?

BETH BACON: Sure. Alan G just [inaudible] and listed six different purposes for auditing. You need to have a purpose for the use of the data, and if we have six purposes for auditing or uses of that data, and no real agreement as to how we're going to keep that either synonymized or anonymized and we aren't really clear as to exactly who will be doing the auditing for what purpose, these are all questions that need to be answered. That was the nature of my intervention.

I don't think there's enough specificity. I don't think I necessarily disagree with logging if we must do it. I don't know why we particularly need this much. I'm all for having ICANN Compliance

have the tools they need to make sure the SSAD is doing what they're supposed to be doing. It's still not clear as to whether the SSAD is going to be doing this auditing originally for potentially abusive requests. I just think we don't have quite enough specificity, and that was the nature of my concern, because it was not clear. Thanks.

JANIS KARKLINS: Okay. Thank you. The principle that logs should be made and then maintained was one of the first that we agreed as part of the overarching architecture of SSAD. So the question is only how detailed those logs should be, and we agreed that there should be some information about accreditation, there should be some information related to requests themselves, and then there should be logged information about responses to the requests and that would be for the purpose of statistics, for the purpose of overall assessment of functioning of the SSAD, and improvements of its functioning, and potential evolution.

So I think it wouldn't be wise to question whether logging is needed or not. So that was agreed and we need to stick with our previous agreements.

Now, the question is—and I would repeat myself, so for the moment, it is suggested that central gateway would perform logging of information related to contents of the query itself and results of processing of the query including the status, and then the suggestion as I understand is also that central gateway maybe should keep logs on disclosure and nondisclosure, use of each rationale for nondisclosure and differences between the disclosure

and nondisclosure decisions of contracted party and recommendations of the gateway.

So from one side, I personally see that this would be useful to have that information, especially if we take into account that central gateway will produce recommendations on each disclosure request. We'll send that recommendation to contracted party and will receive back information whether recommendation was followed or not, and in case of non-following of recommendation, also explanation why in order to train the algorithm that will be used to generate those recommendations. And that, in my view, makes sense that we add those three additional bullet points to this implementation guidance.

But of course, I'm just a moderator of the conversation and it is up to team to decide. Mark SV, please.

MARK SVANCAREK: Thank you. I'm hearing a lot of confusion on the call here. I started developing a data flow diagram for this, a privacy by design data flow and a corresponding DPIA, and at some point, I determined that it might not be useful for this group, so I held back on it. But I think maybe it will be useful. So if it's okay with the group, I'll send that out to the list so you can—hopefully it'll be useful for everybody. Thanks.

JANIS KARKLINS: Thank you. So I do not have any comments on suggested addition to the part which is marked in blue, and so make a proposal

simply to add those three bullet points that are in the question to the logging related to central gateway manager. Any objections?

I don't see any hands up. I take that no one objected. Thank you. Number two, Marika, please.

MARIKA KONINGS: Thank you. Currently, bullet point E says logged data will remain confidential and must be disclosed in the following circumstances. So the first question here is, should "will" be changed to "must" so it reads, "Logged data must remain confidential," because we haven't used "will." We have to either use "must," "should" or some of the other terms that are predefined. And then a related question is, in the second part of the sentence, should "must be disclosed" be changed to "may be disclosed in the following circumstances," or should it read, "must be disclosed where legally permissible in the following circumstances?"

JANIS KARKLINS: Okay. Thank you. So first question to unify approach and use the same determination that we're using everywhere, either "must" or "should," and here we have "will." The intention was to keep log data confidential and disclose it only in certain circumstances. So logic would suggest that we replace "will" in the first sentence with "must." Any objections?

I see no hands up. I take that this is what we can do. Now, the second question is whether in the second part of the sentence, "Must be disclosed in the following circumstances," whether we maintain this or we change it to either "may be disclosed in the

following circumstances" or "must be disclosed where legally permissible in the following circumstances?"

Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. I'm looking at this one and, for example, four, general technical operations to ensure proper running of the system, I think that we don't want to say "must" in all caps "be disclosed to the following circumstances," because it's general technical operation to ensure proper running of the system.

I don't see it as a true statement that looking at the logs is always necessary to ensure the proper running of the system. That's a pretty broad statement. So there, I would think "may" is a better fit. But also, the other point, "where legally permissible," I think that's consistent with language we've used in other sections of the recommendation, so it's probably a good idea to add that here as well. It just seems a little weird to define circumstances where logs must be disclosed. The technician operating the system may not want the logs in all circumstances, so sort of saying, "Well, I have this recommendation that I must give you the logs, so here you go, whether you want them or not," just seems a little weird. I think a "may" is a better fit for what we're trying to accomplish here.

JANIS KARKLINS: So then your suggestion is to reformulate this subpoint E in the following manner: "Logged data must remain confidential and must be disclosed where legally permissible in the following circumstances," and then you have first three points, and that's it.

And then you add additional sentence which says, “Logged data may be disclosed for purpose of general technical operations to ensure proper running of system.” This is what I understand from your intervention.

MARC ANDERSON: No, I would use “may” for all of those. I was just using four as an example. But I don’t think it’s true that the logged data is required in all circumstances all the time. So a “must” doesn’t seem a good fit there.

JANIS KARKLINS: Okay. Thank you. Mark SV, Alan Greenberg, and Stephanie.

MARK SVANCAREK: Marc Anderson is on to something, although I don’t agree with his preferred text. I think what we’re trying to get at is that some logged data must be disclosed under certain circumstances and other logged data must be available under other circumstances. So more specificity would be required to make this as implementation notes so that it’s clear what needs to be available under what circumstances. He's right that you don’t necessarily need to know what the disclosure rates were in order to see if the system were functioning correctly, but you might need to see that under other circumstances. So more specificity. Thanks.

JANIS KARKLINS: Okay. Thank you. Alan G, please.

ALAN GREENBERG: Thank you very much. Yeah, Mark hit on part of what I was just going to say, that if you read this, this implies the whole log must be disclosed. And we're only talking about selected entries in the log or perhaps even parts of selected entries, or perhaps all of the information for all entries, selected information for all entries to look at the overall workflow and load.

So I think it should be a "may" because "must" implies you're disclosing everything all the time, and that's clearly not what we want. And lastly, I would suspect that the "and" in that first sentence should be a "but" because they're really opposite to each other, that it must [remain confidential] but may be disclosed in the following circumstances.

JANIS KARKLINS: Okay. Thank you. Stephanie, please. We do not hear you. So while you're unmuting yourself, the proposal is to replace "and" with a "but" in the circumstances in the first sentence. But then may I also suggest, in light of conversation, that the relevant log data must be disclosed as Alan G suggested that it is not a blanket disclosure but relevant data? And I still maintain the proposition that first three bullet points are very specific and link to audit or legal action.

The fourth is less sort of legal obligated and the logged information maybe disclosed or certain information may be disclosed. So please, after listening to Stephanie, I will formulate the final proposal that we can move on. Stephanie.

STEPHANIE PERRIN: Thank you very much. I am way back at what Marc Anderson was saying about “where legally permissible.” We have indeed used that expression regularly, and I am reminded by the recent correspondence from Göran to the European Data Protection Board that if we stick to that particular formulation, without the caveat of “and in compliance with this policy,” then we will be permitting operators in jurisdictions that don’t have data protection law to ignore things where a data protection authority or the law does not apply.

So I realize it gets extremely cumbersome, maybe it’s a note at the beginning, but I don’t believe we have that note at the moment. So we have “where legally permissible” sprinkled all the way through, and that can permit people to get out of compliance with law. Thank you.

JANIS KARKLINS: Thank you. I think the default situation here is that logged data is not shared, but it must or relevant logged data must be disclosed in very specific three circumstances that team has identified in Los Angeles, and that is first three bullet points.

And then comes the fourth bullet point, which is more general, and that is simply maintenance of the system where logged data may be useful to do whatever fixing needs to be done. So Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. Just noting in chat, I think somebody suggested "relevant." Alan Greenberg, maybe. I think that helps with the discussion we're having. So maybe "logged data will remain confidential and relevant data must be disclosed to the following circumstances where legally permissible." I think maybe that threads the needle.

JANIS KARKLINS: Thank you. Then let me formulate the proposal. First sentence, "logged data must remain confidential, but relevant logged data must be disclosed where legally permissible in the following circumstances." And then first three bullet points. And then the next sentence would be, "relevant logged data may be disclosed for the purpose of general technical operations to ensure proper running of the system."

Margie.

MARGIE MILAM: Hi. I think there's probably other scenarios where the logged data might be published but in an aggregate, perhaps in a report by ICANN without identifying any specific individual data. So I want to just make sure that the recommendation doesn't preclude ICANN from publishing reports based on the logged data.

JANIS KARKLINS: Okay. Thank you. And then remember that there's also two elements. One, we have a footnote which suggests in the second or small roman ii(e), logs should be further available to the data

protection authorities, ICANN, and the auditing body, which says that EPDP team to review at a later stage ability of SSAD to log this information depends on who is the entity that makes disclosure decisions.

So probably, we need to deal with that and take this reference point out. And then also, one needs to remember that we have a reporting requirement recommendation, recommendation 8, which suggests what information will be published in these reports. Alan Greenberg, please.

ALAN GREENBERG: Thank you, Janis. I was going to say something essentially what you just talked about. We do have reporting requirements. Now, if the reporting requirement is getting the data to do the reporting overrides this, that's fine. But for clarity, we probably want another bullet point or another item under this list, under E, saying the data can be used in service of the reporting requirements.

JANIS KARKLINS: So please, could you repeat? I was distracted. My apologies, Alan.

ALAN GREENBERG: Yeah. Sorry. It's fine. It's not clear to me whether the reporting recommendation overrides this, but for clarity, the reporting information will probably at least to some extent be derived from the logs. Therefore, unless it is really clear that the reporting requirement overrides this part, we probably want a fifth item here

saying that the logged data may be used in service or in creation of the reports necessary under the reporting recommendation. It's not well phrased, but I think the intent is clear.

JANIS KARKLINS: Yeah. If I may ask staff to look what is the reporting requirement just to make sure that there is no contradiction in these two recommendations. But again, I would like to rephrase—not propose—the following formulation as a result of this conversation.

So the first sentence would read that logged data must remain confidential, but relevant logged data must be disclosed where legally permissible in the following circumstances.

And then the first three bullet points remain as is, probably with the deletion of reference 22. And then there is another sentence which suggests that relevant logged data may be disclosed for the purpose of general technical operation to ensure the proper running of the system. So that is the proposal. And staff is checking whether reporting requirements are not contradicting with the logging requirements here.

So, can we live with that? No request for the floor, so let's hope that this is acceptable. Number three.

MARIKA KONINGS: So there's a bullet point that reads, "Disclosure decisions including a written rationale must be stored and put in escrow so it can be accessed by ICANN and the contracted parties in case of

objections or legal claims raised to support a legal defense." There was a question or suggestion raised that, should this also include the same latitude for compliance purposes by ICANN, such as responding to complaints, auditing contracted parties and/or enforcing against parties not meeting their disclosure obligations? One way if there's support, and of course, access by ICANN that could include ICANN Compliance that something could be added to the sentence that would read, "and for compliance purposes," or something of that nature.

JANIS KARKLINS: Okay. Thank you. Can we have on the screen highlights of the relevant part of the recommendation? Okay, thank you. Alan Woods, please.

ALAN WOODS: Thank you. I feel like I have to use the Stephanie Perrin line here but, I hate to be like a broken record on this, but this is, again, another example of us absolutely doing far too much and creating a whole issue again for us. This concept of escrow, of what our data and decisions relating to personal data and the personal circumstances of individual registrants, that we have applied to the decision-making process, is kind of pointless.

I think, again, as a disclosing body, I would keep the rationale myself as a controller and I would have that retained in my own system for a period of time so that I could prevent, again, as [I] said there, if there was somebody to sue us or there was a complaint made, so I could respond to that. I don't understand

why ICANN would need the rationale, because again, this whole point of ICANN Compliance and enforcement—which we were talking about the last day even—is about the procedure, not about the decision itself. And at this particular moment in time, the way it is set up, I would not be comfortable giving ICANN or placing this rationale or this decision-making in any escrow, because again, assuming placing it in an escrow is potentially having another party in which we're processing our data on our behalf for no reason, because we again hold that data, and it is accessible in the event of a complaint or a legal case has been raised.

So there's, again, a lot of duplication here, a lot of unnecessary processing of data, the transfer, again, misunderstanding of ICANN's process in place, I personally believe. And I think we should never be even considering escrow. That is up to the individual controller to have and to hold—[inaudible] somebody now—but like it just makes no sense to me why we would escrow this data.

JANIS KARKLINS: Okay. So if that is in the initial recommendation, that means we had a conversation and agreed to put it in the initial recommendation. So I do not recall specifically this section of our conversation, but certainly, there will be voices speaking in favor of this proposal.

Nevertheless, it is maybe not good at this stage to say that this does not make sense, because it is our own proposal and initial recommendation. Mark SV, please, followed by Alan Greenberg.

MARK SVANCAREK: Thank you. I too do not remember why we say that the controller must store and also put it in escrow. I don't remember why we agreed to that redundant storage. So we should try to figure out why we put that in in the first place, because as I'm looking at it, I don't see the point of it. Thanks.

JANIS KARKLINS: Okay. Alan G.

ALAN GREENBERG: Thank you. I tend to agree. The wording implies that ICANN may want to access the reason that the contracted parties did something. But I can only see that in edge cases if the contracted party has ceased to exist in the interim. And I'm really not sure that handling that kind of edge case makes it worth doing something as massive as putting all of this data in escrow. Thank you.

JANIS KARKLINS: Okay. If I understand correctly then, no one can remember why it appears, author is not manifesting him or herself, and I do not have any notes from staff, which means that we can delete it. Can we? Chris Lewis-Evans.

CHRIS LEWIS-EVANS: Thank you, Janis. Yeah, I think we can delete it, but only from the word "stored." Everything forward of that, I think we can delete,

the disclosure decision and the written rational must be stored, just leave it at that. Thank you.

JANIS KARKLINS: Okay. Alan G.

ALAN GREENBERG: Thank you. When you say “it,” do you mean the escrow reference, or that whole sentence?

JANIS KARKLINS: No, Chris just clarified.

ALAN GREENBERG: Sorry. Chris wasn’t loud enough, I couldn’t quite hear him.

JANIS KARKLINS: Yeah. the part of the sentence that starts with “and put in escrow,” so Chris suggested that the part of the sentence, “disclosure decisions including a written rationale must be stored,” full stop.

ALAN GREENBERG: And would you want to continue with “in case of objections?”

CHRIS LEWIS-EVANS: No, I don’t think so.

ALAN GREENBERG: Okay. Not an issue for me anyway.

JANIS KARKLINS: Okay. So proposal is to delete the part of the sentence starting with “and.” Berry, if you could indicate that. Starting from, “and put in escrow,” so this would be deleted. Alan Woods, are you in agreement?

ALAN WOODS: I'm generally in agreement. I just think we need to be careful that what we’re creating there as a potential recommendation is exceptionally broad. Must be stored by whom and for how long is what we’re kind of missing there.

JANIS KARKLINS: No, we’re not, because it is recommendation related to contracted parties.

ALAN WOODS: Okay. Sorry. Fair enough. But then by how long? Again, knowing the trouble that IRT have gone through in phase one, it might be helpful for them to point out it should be up to the individual disclosing party to set the relevant retention periods based on their own company jurisdiction, things like that.

JANIS KARKLINS: We have retention recommendation and probably that logging information would be covered by data retention requirements, no?

ALAN WOODS: It could be, but again ...

JANIS KARKLINS: If I may ask staff to check it.

ALAN WOODS: Yeah, the thing is, or my point is that specificity is probably better here just to avoid long conversations about this having to be logged in the central gateway at IRT level. Just be clear, I think, is important.

JANIS KARKLINS: Okay. So in principle, there's no objection to deletion of this part, and then staff will check if this is covered, how long the logging data should be retained, whether that is covered by data retention recommendation, and if it is, it will stay like that. If not, staff will add the sentence or part of sentence related to length of storage similar to one which we have in data retention recommendation.

So I have no hands up, so I take that this is something we could live with. Thank you. Number four, Marika, please.

MARIKA KONINGS: Thanks, Janis. Number four, there was a suggestion on whether the logging requirements should be simplified, providing the logging entities more flexibility to follow relevant data protection law while also maintaining records sufficient to demonstrate

compliance with the SSAD recommendations and related policies. Suggestion was made that maybe it would be sufficient to only keep the implementation guidance section as the policy recommendation here, and remove the preceding requirements.

JANIS KARKLINS: Okay. Thank you. So, any reaction? My feeling is that that is not really good. Anyway, I'm in your hands. Margie.

MARGIE MILAM: I agree. I think we've already done a lot of work in detailing the logging, and I think it's better just to leave it the way it is since we've already fully negotiated those.

JANIS KARKLINS: Okay. Thank you, Margie. So, shall we keep as is? Of course, with the modification that we have already introduced. Okay, no hands up, I take that this is what we want to do. Thank you. Number five, please.

MARIKA KONINGS: Thanks, Janis. I think the second part of this question has basically been addressed as we already removed the reference to escrow, so it's only the first part of the question, should expansive logging requirements be considered further?

JANIS KARKLINS: Brian, please.

BRIAN KING: Thanks, Janis. I think that to the second sentence there, if we just agreed that we wouldn't need escrow for this, then perhaps that eliminates the concern.

JANIS KARKLINS: No, we agreed already, we took it out.

BRIAN KING: Right. Thanks, Janis. So my thought there is that if we agreed on that, then perhaps we don't have this concern anymore. Thanks.

JANIS KARKLINS: Okay. Thank you. Alan G.

ALAN GREENBERG: Yeah, thank you. Logging is an inherent part of any processing operation, whether it's privacy related or anything, if you're building a reasonable system. So I don't think the question of who bears the cost is relevant, it's just part of the base and any core system. Thank you.

JANIS KARKLINS: Okay. Thank you. So with that understanding, we can move to number six.

MARIKA KONINGS: Regarding to point B, logs will include a record of all queries and items necessary to automate any decision made in the context of SSAD. The question here was raised, is decision auditing the proper goal, or should it instead refer to auditing adherence to the process as outlined in the report? And this may go to previous conversations we had, and this may have been a leftover of of course earlier conversations on where decisions would be made, so this may be an easy fix as adherence to the process instead of referring to decisions here. I don't know if that's an easy way forward on this one.

JANIS KARKLINS: Brian, please.

BRIAN KING: Thanks, Janis. I thought I was going to answer that question one way, then Marika made me second guess it, which I think is good. So in principle, the logs should include the rationale for the decision, but I think we do have that captured somewhere else. So maybe while it is important, we do need it, is that captured somewhere else sufficiently for us? And if we're not capturing it in logs, I guess, why not?

JANIS KARKLINS: Thank you. No, I think it is. Even here, we just finished the conversation that contracted parties will log disclosure decisions, including written rationale must be stored. So it is captured. So, Alan G, please.

ALAN GREENBERG: Just to note—and I'm not sure how relevant it is here, Your reference to contracted parties, it is conceivable that the SSAD itself may be making decisions and those and its rationale will have to be logged as well. So let's make sure we're not just limiting it to contracted parties' logging. Thank you.

JANIS KARKLINS: Thank you. On the central gateway, we added three bullet points. One is divergence between disclosure and nondisclosure decisions of the contracted party and the recommendations of the gateway. So that is indirectly implies central gateway's covered.

So can we here then reformulate that logs include a record of all queries and all items necessary to audit any adherence to process or policy made in the context of SSAD? Hadia, please.

HADIA ELMINIAWI: Thank you, Janis. Yes, I think what we're looking for is auditing the whole process of the request starting from the very beginning until the end. So I guess that's what the recommendation needs to capture, the whole lifetime of the request starting from when the requestor made the request until the decision and the data is disclosed or not.

JANIS KARKLINS: Thank you. So you're in agreement that decisions should be replaced by adherence to the process in the context, or decisions

made should be replaced with adherence to the process in the context of SSAD? Any objections? Thank you. Number seven, Marika, please.

MARIKA KONINGS: Number seven relates to item D, which currently reads logs must be retained in a commonly used, structured, machine readable format accompanied by an intelligible description of all variables. And the question is, is that really necessary? Some suggested that in other cases, ICANN allows each contracted party to make their own determination about the best way to keep logs. Should this requirement be removed as a result?

JANIS KARKLINS: Thank you. So I would say since we're talking about the standard or standardized approach, then it would make sense to keep granularity that everyone does the same. And I think that the current formulation is going in that direction. But of course, if the team thinks it can be different, I'm in your hands. Brian, please.

BRIAN KING: Thanks, Janis. I'm inclined to agree with you. I think this language does allow for a great deal of flexibility already, and I think this is probably what we need. Thanks.

JANIS KARKLINS: Thank you. So, any objection retaining as is, as recommended in the initial report? Alan Woods, please.

ALAN WOODS: Thank you. Just something that Brian said there made me kind of pique my curiosity. So, are we reading “commonly used” as being something that is common, not something that is common to all? That is not going to be standard, it’s going to be something that is just machine readable in general? Because if that’s the case, fair enough. I can't really stand in the way of that.

But again, if we are saying that it must be in a specific way, let’s look at the monster which we’re creating where this would need to be audited and verified and ensuring that everybody is using the same format, and going all different things—again, for very limited use. So again, there's a better use of resources than creating a new logging standard. As long as it is just machine readable, that should be fine.

JANIS KARKLINS: Okay. Thank you, Alan. Alan Greenberg, please.

ALAN GREENBERG: Thank you. I tend to agree with Alan that, yes, this may need to be audited, but auditing firms are well versed in using different tools as necessary. So I think this is overkill, and I specifically think the word “structured” is overkill. If “structured” means there should be fields in an entry, that’s fine. If structured means in the terms of database design, that it’s indexed and complex structure, I think that’s probably overkill. So I would remove the word “structured” here. The rest of it, I think, is fine.

JANIS KARKLINS: Okay. Thank you. So I think that the meaning here is that this is done in the similar way by all contracted parties, and commonly used most likely is existing standard of logging information. Machine readable, structured, again, have no specific opinion, but the point here is that everyone follow the same kind of standardized approach.

Okay, so I see that there is support to delete “structured,” and retain “commonly used machine readable format.” And that would be with understanding that “commonly used” is already existing. It’s not newly developed, but already existing. So, would that be acceptable? No hands up, so it’s so decided. “Structured” goes.

Last question, Marika.

MARIKA KONINGS: Yeah. So question eight, I think we probably already addressed that one. It basically asks if all personal information has been removed from the logs, are there any concerns about making logging information publicly available. And I think we've already discussed that the logging information would be used in the context of reporting. So, not sure if there's any further input on this one.

JANIS KARKLINS: No. Okay. Thank you. We have then finished examination of outstanding issues of recommendation 17 on logging, and I would suggest that we move to recommendation 18 on auditing. We

have remaining 15 minutes in this call, so we could certainly start conversation. Marika, please.

MARIKA KONINGS: Thanks, Janis. So here also, we have a couple of assumptions, takeaways that we took away from the input that was provided by those that provided their responses. First of all, there was a suggestion that—and there was also a question from several, the timing of audits, and there was a suggestion to have audits yearly for the first three years and then every two years following, similar timeline for identity providers.

There were some minor edits that no one expressed concern to that will apply in the next version of this recommendation. There was also the notion that, should audit information include personal information, an information request by the auditor is expected to be processed in compliance with applicable laws. And similarly, in case of data breach that would be detected through an audit, the notification requirements to subjects whose data may have been compromised will need to follow applicable laws and requirements. That would be at least our understanding.

Also emphasizing or clarifying that repeated noncompliance by an accredited entity may result in suspension or termination of the accreditation by the accreditation authority. And there was a suggestion that the results of audits should be published, including the deficiencies identified as well as steps taken to address those deficiencies should be reported. That was also something that was supported by all, so that is something that we'll update in the next iteration.

So there were a couple of items where not everyone agreed or agreed that it should be further discussed by the group. So the first one is we noted that compliance concerning suspected systemic abuse by contracted party has already been addressed in recommendation 8, but one of the questions was raised whether ICANN Org should also proactively audit contracted parties to be able to detect this type of behavior.

So again, number eight, it's a complainant that can flag to ICANN Compliance that they suspect that there's systemic abuse going on, following which ICANN Compliance would investigate, but the question here is, should ICANN Compliance also do that proactively through the auditing process?

JANIS KARKLINS: Thank you, Marika. The question is on the table. Any feelings, any guidance? Brian and Alan Woods in that order, please.

BRIAN KING: Thanks, Janis. I think they should, but is that what consensus policy does? I think what we're building here is compliance requirements for the contracted parties, and I guess we could ask Compliance to do that, but is that [inaudible] ICANN to enforce its contracts? Thanks.

JANIS KARKLINS: Thank you. Alan Woods, please.

ALAN WOODS: Thank you. I suppose there's a lot of already safeguards in there which are in a way detrimental to the contracted parties as in they're additional elements that are being layered on on this one. And again, it's a question of whether or not ICANN Compliance's time and resources could be better used.

The thing is that it's a very hard thing to test. We've got SLAs, the SLAs will be monitored. We got complaints, complaints will be monitored. What are they supposed to do, go in and pull ...? Again, this is a consensus policy, so they're going to have to do it anyway. I just think, again, we're over egging, and we should just keep it the way it was and not continue down this particular route at all.

JANIS KARKLINS: Okay, so I see that there is common understanding that if there are complaints, or indications that there is systemic abuse, of course, then it should be addressed by Compliance, but Compliance itself should not proactively reach out and seek whether there is something or not.

Mark SV, please.

MARK SVANCAREK: Thank you. The SLAs proposal already says when ICANN will do their audits. That's already defined. So I think this wording is probably redundant. But I would point out that the system envisaged by the SLA section is constantly generating statistics on a running basis, and if ICANN wanted to put an alert in the system to let them know that somebody has crossed a specific

threshold and therefore should be further scrutinized, that would be basically free and wouldn't require any extra effort on their part to monitor.

So when we get to the SLA section, we can talk about whether or not we want to include proactive or ongoing monitoring as part of the system, but I assume that we didn't. Thanks.

JANIS KARKLINS: Okay. Thank you. So then with that understanding, we move to next question.

MARIKA KONINGS: So question two relates to the audits of the accrediting authority, and recommendation currently states that ICANN Org as the accreditation authority is not required to audit governmental entities whose accreditation and audit requirements are defined in preliminary recommendation number two.

if ICANN Org is not the accreditation authority, would a third-party accreditation authority be required to audit governmental entities, or would any accreditation authority be exempt from auditing governmental entities? What is the rationale for this, and for any distinction in auditing requirements as between ICANN Org versus a third-party accreditation authority when it comes to auditing governmental entities? And just to know that recommendation 2 is still under review by the GAC team, although I don't think there were any specific changes foreseen to that aspect of the recommendation at this stage. But they may be able to speak to that.

JANIS KARKLINS: Okay. Thank you, Marika. So now, the GAC group is on the spot. And I would like to see all three hands up. None? Chris, please, go ahead.

CHRIS LEWIS-EVANS: Thank you, Janis. So in the recommendations, it was clear that the government accreditation authorities would have to have auditing available, so I thought that was already covered in there, and they wouldn't be necessarily audited by ICANN, there would be a proper auditing process, and obviously, that would be made available to ICANN.

So I seem to think that was covered in there, and as Marika says, the new version isn't any different. So unless anyone else thinks otherwise, I think this is already covered.

JANIS KARKLINS: Okay, but we have not seen the new version. Not yet.

CHRIS LEWIS-EVANS: No, not yet.

JANIS KARKLINS: When?

CHRIS LEWIS-EVANS: It's in a final version, it's just waiting signoff currently.

JANIS KARKLINS: Okay. So then hopefully, the new version will cover that question. And in essence, Chris, if I understand correctly and also if staff understands that in the new version, there will be auditing option for the accreditation of government authorities, but not by ICANN but by the commonly defined entity, right?

CHRIS LEWIS-EVANS: That's right. That was in there in the first one, I believe.

JANIS KARKLINS: Okay. So we are impatiently awaiting revised recommendation on accreditation of government entities, so that's all I can say. Thank you. Let us go now to point three.

MARIKA KONINGS: Thanks, Janis. So three is similar to what we discussed previously, and I don't know if the response here is the same, but it asks about whether the expense of auditing requirements should be considered further and incldued in the final report. Just to note that I think on the previous similar questions in relation to logging, people noted that it's part of the nature of the beast. If you have a recommendation, there is a logging that takes place, as well as auditing, and there may not be any need to further elaborate on that. But again, I give that back to you.

JANIS KARKLINS: Okay. Thank you, Marika. So the understanding is that auditing is the part of operational cost and it should be seen like that. Is there any dissenting views in this relation? I see none. Let us move now to number four.

MARIKA KONINGS: Number four was a notion that there are already a number of auditing requirements that are contained both in the registry agreement as well as the registrar accreditation agreement. And for completeness, you can actually find those sections further down in this document. So the suggestion was here, is it necessary to include all these auditing obligations, or should a further effort be undertaken to only include those auditing obligations that do not already exist under relevant data protection laws and are not covered yet by those requirements?

I think as we also discussed previously, if there are any updates that are required to the registry or registrar agreement as a result of these recommendations, that is something that would basically automatically happen or there would be a cross check. So maybe any duplication is not necessarily an issue. But again, I think this was a suggestion to potentially try to simplify this and only add those specific requirements that are not already called out in those sections that are referenced here.

JANIS KARKLINS: Okay. Thank you, Marika. Berry, could you outline which part of the recommendation we're talking about? I think that should be lower, it's about audits of accredited entities and individuals.

Any opinion whether this section should be somehow simplified or should be kept as is? With understanding that even if this is already envisaged in agreements, the registration agreements and accreditation agreements, that we simply leave it as is. Margie.

MARGIE MILAM: I would propose leaving it as is. I think it actually is more of an implementation issue to look to see how it gets implemented and whether it's already covered. But I think it would be confusing to have to go now and figure out what's there and what's not there, and then the implementation team won't really understand that we intended to keep it all there. So I would just leave it as is.

JANIS KARKLINS: So Margie suggests to leave as is, and draw conclusion to this call today. Okay, no objection, so we leave the recommendation as is in the respect of the context of question four.

So thank you very much. I think we have made good progress today. Of course, it was very full agenda and I had no illusions that we would get to the end of suggested agenda. We will continue on Thursday starting with question five from auditing, and we'll continue with implementation guidance, and also, most importantly, with financial sustainability and evolution mechanism.

In that respect, I would ask those groups who have not reacted to these two recommendations to do so in expedited manner, that we can have a good conversation. And then next Tuesday, we would attempt to talk about priority two issues.

So with this, I would like to thank once again all of you for active participation, and draw this meeting to the end. This meeting is adjourned. Have a good rest of the day.

TERRI AGNEW: Thank you, everyone. Once again, the meeting has been adjourned. Stay well, and chat everyone later this week.

[END OF TRANSCRIPTION]