ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Tuesday, 24 September 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/EJACBw
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 meeting taking place on the 24th of September 2019 at 14:00 UTC.

In the interest of time, there'll be no roll call. Attendance will be taken via the Zoom room. If you're only on the telephone, could you please identify yourselves now?

Hearing no one, we have listed apologies from Allan Woods, RySG, Brian King, IPC, James Bladel, RrSG, Stephanie Perrin, NCSG, Hadia Elminiawi, ALAC, and Marika Konings from staff.

They have formally assigned Sean Baseri, Jennifer Gore, Owen Smigelski, and Holly Raiche as their alternate for this call and any remaining days of absence.

Alternates not replacing a member are required to rename their line by adding three Zs to the beginning of their name, and at the end in parentheses, their affiliation, dash, the word "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 assignment form. The link is available in all meeting invites.

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 need assistance updating your statements of interest, please e-mail the GNSO secretariat. All documentation and information can be found on the EPDP Wiki space.

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

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

JANIS KARKLINS: Thank you, Terri. Good morning, good afternoon, good evening, team members. Welcome to the 20th meeting of the team, and I now would like to see whether we can work according to suggested agenda as it’s now displayed on the screen. Any comments?

I see none, so I take that we can fallow this agenda with understanding that indicated time is simply for indication and we may use more or less time depending on the progress of our conversation.

With this, let me move to agenda item three, housekeeping issues. There are three issues instead of two. The first is in Los Angeles, we agreed that as a homework, each group would look at the table on lawful bases for disclosure, and do their inputs in that table by Wednesday 25 which is tomorrow so that we can look to the results of this work during our next meeting in coming Thursday.

So, any questions of this homework or any comments? None then. On subpoint B, Terri, would you take it?

TERRI AGNEW: Thank you, Janis. I'll actually turn it over to Caitlin, I believe. Caitlin?

JANIS KARKLINS: Okay. Caitlin.

CAITLIN TUBERGEN: Thank you, Janis. Would you like me to read out the additional outstanding action items from the face-to-face meeting?

JANIS KARKLINS: No, first was about the submission of alternate forms for the face-to-face meeting end of January.

CAITLIN TUBERGEN: Thank you, Janis. Apologies.

JANIS KARKLINS: Terri, that was your topic.

TERRI AGNEW: Yes, it was. So sorry about that. I went to a completely different B. So if I could just remind everyone to please complete the alternate form if you are not able to attend the January 2020 face-to-face meeting. An e-mail invite has been sent as well as the reminder e-mail with the alt form, and again, as a reminder, the alternate form is in every single meeting invite towards the bottom.

We are going to be submitting travel for everyone this week by the end of the week, so if you're not able to attend, please complete that form so we know not to submit travel for you. Thanks, Janis. Back to you.

JANIS KARKLINS: Thank you, Terri. And now Caitlin, if you could walk us through the remaining or outstanding homework that we need to complete.

CAITLIN TUBERGEN: Thank you, Janis. You'll note that in the chat, I pasted a link to an e-mail that Marika sent last week that organizes all of the outstanding action items from the face-to-face, and I wanted to quickly go through these as I believe all of these are still outstanding.

The first was for Alex Deacon, Milton Mueller and other willing volunteers to draft up a potential accreditation model taking into account the feedback we received during the face-to-face. Secondly, we have IPC, BC, SSAC and GAC reps to separately draft a vision for their ideal accreditation model. That was due last week.

Next we have – which I believe Janis mentioned earlier – the lawful basis table for the EPDP members to populate their feedback in, and that feedback is due tomorrow so that we can prep for Thursday's meeting. We also had as an action item for EPDP team members to populate the disclosure decision model table, and I believe thus far we've received feedback from the IPC, the Registrar Stakeholder Group and ALAC. That feedback was due last week.

Next we had EPDP team to review the legal memos that everyone received during the face-to-face and note any relevant points that they believe to be factored into our further discussions.

As we discussed last week, James and Mark SV are working together on a revised proposal for building block L, the SSAD query policy. Matt C is to review the legal advice on how to perform a balancing test and update Alan Woods' initial balancing test document into a guide for how to conduct a balancing test.

And lastly, we have the contracted party team members to draft a letter to the ICANN board outlining scenarios discussed, including where the disclosure decision lies within the SSAD and inquire whether there are any options the board would not be amenable to. And again, I did paste a link to this e-mail into the chat so everyone can review it on their own screen. Thank you, Janis. Back over to you.

JANIS KARKLINS: Thank you, Caitlin, for walking us through and reminding folks. I would like to ask you maybe during the call or immediately after, simply drop a short line to me or Marika indicating where you are with the homework, because essentially, we need to know because that is linked to the planning of our meeting. So specifically for next Thursday we're hoping that two homeworks will be done on accreditation and query policies, that that is on the schedule for next meeting, as you know from the suggested timetable of activities until Montréal. So please let us know, and if I may encourage you to do the homework as soon as feasible. Any comments, questions?

I see no requests for the floor. Let me then move to our substantive agenda item, and that is acceptable use policy, building block D and H. So together with the agenda, we circulated respective parts of the zero draft and we will be using them for our conversation.

The acceptable use policy actually consists of two building blocks; one related to request and another related to reply. In this respect, zero draft formulates five subpoints that you see now on the

screen as well as in the box you see comments that have been provided by different groups in the run up to face-to-face meeting that contains certain proposals and we would go through also one by one, not only suggested subpoints but also comments and concerns. And then of course, everyone is free to propose new ideas that are appropriate for the sake of conversation.

And if I may suggest that we start with the demand side and then go to supply side. Would that be okay? Seems to me the case. Let me then ask if there is anyone who wants to comment on the use policy. If none, then let us take subpoint by subpoint, subpoint A and the text is the overarching text or chapeaux text, EPDP team recommends that the following requirements to the requestor and must be confirmed and enforced by depending who is in charge. So must only request data from the current RDS data set. No data about the domain name registration history. Margie, please. Your hand is up.

MARGIE MILAM: Good morning, everyone. Actually, Janis, I wanted to go up to the introduction and suggest the deletion of the words “and enforced by.” I think the concept is that we’ll talk separately about auditing but the notion that each request is somehow enforced or each data request would be looked into. It’s, I think, not appropriate in the circumstance. So I suggest we have a separate section that deals with the auditing and what that means, but anything that relates to tracking what a specific request is would be problematic.

JANIS KARKLINS: Okay. Thank you, Margie. Any objections to Margie's proposal? I see Volker's hand is up and also his comment in the chat room. Volker, please go ahead.

VOLKER GREIMANN: Yes. I think we're not looking at individual requests. We're looking at requirements that the requestor has to meet and that he has to confirm. And these requirements have to be enforced, otherwise without enforcement, there is no meaning to have any requirements.

So I think the enforcement part is important and should be maintained. It does not mean that every single request has to be reviewed and enforcement reviews have to be carried out for each and every request, but there has to be an enforcement mechanism that can be triggered in case of apparent misuse or suspected misuse.

JANIS KARKLINS: Thank you, Volker. Margie, do you agree? While you're thinking, Mark.

MARK SVANCAREK: Margie will probably say the same thing as me. I'm also concerned about this enforced language, but I would suggest that perhaps Volker put forward some alternate language that we could all agree on. Thanks.

JANIS KARKLINS: Yeah. Margie, are you in agreement with Mark?

MARGIE MILAM: Yeah, that's fine. I understand the obligations need to be something that are generally enforced, but this implies that it's specific to a request. So we could take that offline, that would be terrific.

JANIS KARKLINS: Yeah, let's put this "and enforced by" in square brackets and then we'll revisit that or we'll think also maybe with staff if there's any alternative, or you could come up with any alternative that you may think of online and we will revisit it in the second reading.

Okay. First, subpoint A, only current data, no history. Proverb goes though if you do not know history, you cannot build [the past.] Take it as a joke. Not relevant to this topic. Any requests, any comments on this? Chris Lewis-Evans, GAC.

CHRIS LEWIS-EVANS: Thanks, Janis. I know [inaudible] it's just whether we need to change language slightly, because when the domain was fist registered, it's something about the domain's history, but that's not what this is trying to cover off. This is trying to cover off historic data. So no historic data about the domain name I think would be better for me rather than the language there. Thank you.

JANIS KARKLINS: Thank you. I think they're meaning exactly that, what you mentioned, that no access to historic data but only to current. That's the meaning of the point. I think that staff noted that and it will be changed for the future, for the second reading, unless anyone objects. I see none. Any other comments on subpoint A?

So then subpoint B, must provide representations with each unique request for data or of its corresponding purpose and legal basis for their processing, which will be subject to auditing. And in the brackets, no bulk access.

And actually, related to this, there was one comment suggesting that considering including reference to registration accreditation agreement, defining bulk access from section 3.3.6. I see two hands up. Chris Lewis-Evans first, followed by Margie.

CHRIS LEWIS-EVANS Thanks, Janis. I think it's quite good language. I really don't see the need for the no bulk access in there. If it is, yeah, I think it just needs some highlighting that refers to that language. I really don't se the need, it's quite tight as it is. Thanks.

JANIS KARKLINS: So you suggest to take out "no bulk access" from brackets? Am I right? Chris? Are you there? Okay, Margie, your hand was up.

MARGIE MILAM: Sure. I agree with what Chris just said, that there's no read for the reference to "no bulk access," but if there is a reference to it, then

you need to include the citation because I think it makes sense without it.

JANIS KARKLINS: Okay, so any objections of taking out bulk access, striking bulk access in brackets? Volker?

VOLKER GREIMANN: Not an objection. I think the language is clear, but the bulk access was basically intended there as a reference of what was meant when we said when we said we would have unique requests for data. So it should be somewhere in the annotations that that was the intent of that language to make sure that it's not lost. But essentially, the language can be cleared up for easier understanding, so I don't object to that specifically.

JANIS KARKLINS: Okay. Thank you, Volker. We will then try to work with staff to see whether clearer formulation underlying that each request should be – there should not be clustering of requests but each request is unique, and we'll see how to present that clearer than it is currently in point B. I see Alan's hand is up. Alan Greenberg, please go ahead.

ALAN GREENBERG: Thank you very much. Again, I mentioned the last time, the term "bulk access" seems to be used in multiple ways, and for that alone, I would suggest not using it.

If what we mean is you can't put three different requests on the same thing even though all the other information is clear, I'm not quite sure of the benefit of that, but I don't really care. One obviously can automate any requests to send three at once with different names, but I think we need to be really clear so there's no confusion.

Certainly, this means no wild characters in a request. I'm not sure it makes a lot of sense to say you can't submit three requests in the same packet, but I'm not the one who submits requests so I'm not going to argue very strongly for that. Thank you.

JANIS KARKLINS: Thank you. As I said, we will try to propose maybe slight clarification in the next edition. But the meaning is that each request is unique as it is in the first one.

Okay. No further request? Let us then go to subpoint C. Must only use the data for the purpose requested. No fishing around, in other words. Alan, your hand is up, or that's the old hand? It's old hand. Alex Deacon.

ALEX DEACON: Hi. Good morning. I think this comment is ours. I believe that we consider updating C to state "must represent that requestor will only use the data for the purpose requested," and then we also believe that covers what is currently in E, so E could be deleted .Thanks.

JANIS KARKLINS: Could you please repeat the proposal? Please go ahead.

ALEX DEACON: Sure. So we're suggesting updating C as follows: "Must represent that the requestor will only use the data for the purpose requested."

JANIS KARKLINS: But that is already what is written here. If you take together "Recommends that following requirements applicable to requestor, so requestor must use the data for the purpose requested."

ALEX DEACON: I see. Yeah. And then we suggested that E would be redundant and that we should delete E.

JANIS KARKLINS: Okay. So there are two proposal, basically proposal is taking into account the substance of subpoint C to delete subpoint E. I see Amr's hand is up, and Alex, you probably need to lower your hand. Amr, please go ahead.

AMR ELSADR: Thanks, Janis, and thanks, Alex. I'm just curious about the intent in this proposed edit to C. What's basically being proposed here is that the only requirement is that there will be representation that the data will be used for the purpose for which it was requested

but actually using it consistent with that purpose is no longer a requirement. Am I getting that right?

JANIS KARKLINS: No, I think that what you see on the screen is not exactly what Alex was proposing. So we're not changing anything in subpoint C.

AMR ELSADR: But point C was about the actual use of the data, it wasn't about representation of the use; right?

JANIS KARKLINS: No, we're not changing –

AMR ELSADR: Oh, alright.

JANIS KARKLINS: The meaning of subpoint C is that requestor must use only data for the purpose requested.

AMR ELSADR: Right, and I'm fine with that. Yeah.

JANIS KARKLINS: Yeah. So now it's the auditing part. We could maybe think to combine subpoint C and E suggesting "Only use data for the

purpose requested which might be subject for auditing" or something like that. That was basically idea that Alex proposed, and then we would delete subpoint E. Amr?

AMR ELSADR: Okay.

JANIS KARKLINS: While you're thinking, I'm keeping you in line. Alan Greenberg, please.

ALAN GREENBERG: Thank you. I think they're both needed, although they could be merged, but the order is wrong. The current E says in the request you must say what you plan to use the data for, and C says "And you must follow through and only use it for those purposes." So I think perhaps once you've said what you plan to use it for, that implies that's all you must use it for. If we want to be really tight, then we need both of them but in the right order. Thank you.

JANIS KARKLINS: Okay. Thank you, Alan, for the suggestion. I'll take Chris, and then Alex, would you agree with Alan's suggested change of sequence, putting E before C? Chris, please go ahead.

CHRIS LEWIS-EVANS Yeah, thanks, Janis. I was about to agree with Alan, actually. If my memory serves me right, the purpose of C here is one of the

principles within GDPR that you can only use personal data for the legal basis and the purpose you quoted when you actually obtain it. So I think that's what C was trying to cover. E I think is trying to actually cover the necessity principles that will ask for the data, and that would be subject to the purpose plus the legal basis. So as a requestor, I'd have to provide that sort of information when requesteing data. Obviously, that would be subject to auditing and that audit would be to see whether or not I had maybe used that data only for the purpose requested and why I was doing it.

So I think they both need to be there, and I would agree with Alan, maybe swapping the order around. Thank you.

JANIS KARKLINS: Okay. Thank you, Chris. Alex, would you agree to lift E before C and maintain it?

ALEX DEACON: Yeah. Hi. I think I need to read it from top to bottom. I wouldn't object to that at the moment. I think really, as we touched on earlier, it really depends on what we mean by auditing and what context this happens and how it's triggered and so on. So there's still a lot of work to do there, I think, under the covers. Thanks.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: Sure. I want to also point out something that's a little problematic with the word "only," because there are situations where you're investigating, say, a cybersecurity event, and it could also be a trademark infringement if it uses a domain name that has your brand in it, just to give you an example.

So I think it has to be – only use it for purposes consistent with the request, but it shouldn't be so strict that if you say trademark infringement and you use it for cybersecurity, that somehow there's a breach of the representation. So the word "only" in this case makes it seems as though you have to basically list out every potential purpose that the data could be used for as it relates to the request, and I think that that's probably a little too strict.

JANIS KARKLINS: Thank you, Margie. I'm very distracted with that Porsche where the license plate is not seen. Can we get – thank you. Alan, your hand is up.

ALAN GREENBERG: Yeah, thank you. I forgot what I was – sorry, your comment about the Porsche made me forget. Let me see if I can bring it back quickly.

JANIS KARKLINS: Okay, so Margie was proposing to delete "only" in a new subpoint D. Any objections, reactions to that? Amr?

AMR ELSADR: Thanks. I don't think it's a good idea to get rid of that word. Margie, you use trademark infringement and couple that with the cybersecurity as two examples, but the point here is that in order to be GDPR compliant, you have to be clear on the purpose for which the data will be processed and then you need to match that along with the corresponding legal basis. And then those need to be clearly outlined before the data is processed.

Now, using trademark infringement and cybersecurity are two good looking examples, but keeping that word, "only," there also ensures that if someone is requesting the data, let's say, for the purpose of trademark infringement, then decides to use or process the data further for any other reason besides cybersecurity or trademark infringement which may not be compliant with data protection law, then getting rid of "only" here in our policy recommendation allows the party to actually go ahead and do that.

I don't think we need to list every single potential purpose here and just have a blanket statement saying that the data requestor can process this data legally for purposes one through ten. I think we do need to be very specific and that the data requestor, once they have their hands on the data, they need to only process it consistent with the purposes that they spelled out. Thank you.

JANIS KARKLINS: Thank you, Amr. Can we think something along the lines saying that we maintain only but then add at the end of the subpoint

statement along the lines –and now I'm really talking from top of my head – suggesting if during whatever processing or investigation, it appears that, and then the requestor or the – sorry, if during the investigation appears that requested data could be used for other purpose, then that should be made known to contracted party or something like that. I'm just speaking top of my head now.

Alan, have you remember what you want to say?

ALAN GREENBERG: I did remember, and I also have a comment on the “only.” Several people in the chat and in fact Amr in his final sentence said if you can only use it “for purposes consistent with ...” And Chris also used the word “incompatible,” not use it for things that are incompatible.

So I think either by the use of “compatible with” or “consistent with,” we can cover both cases. So I think that addresses the problem well enough, and I certainly, in anyone’s mind, if as you're investigating one thing, it leads to another ,and this happens on a regular basis. I think that’s [inaudible] “compatible with” or “consistent with.”

The reason I originally put up my hand was on the auditing term. I'm very uneasy about saying that anyone who requests any data is then giving blanket permission to be audited by some unknown agency with no limits on what they're allowed to audit or how they're going to audit it. If I was a company, essentially that says I'm going to open my complete books to anything for someone to

fish around or try to see how I use the data, it's just too open ended. So I think if we use the term "audit," we have to have a large footnote somewhere explaining exactly what we mean. Thank you.

JANIS KARKLINS: I think we have one of the building blocks referring to auditing, so that will be described there. But your concern is noted. Margie, followed by Mark and then Volker.

MARGIE MILAM: Sure. Thank you. I suggest we use the language from GDPR section 5(b) and I put it in the chat. Basically says that would not be further processed in a manner that's incompatible with the purposes cited. So if we do that, then I think that addresses my concern.

JANIS KARKLINS: Okay. Thank you. [Berry,] you have captured that, right? Mark.

MARK SVANCAREK: Hi. As a general statement, I'm uncomfortable with the idea that we are trying to rewrite privacy law into this policy, because we're going to be using different terminology and different structure than is in the data protection laws. So we'll just wind up with some weaker mutant version that is pretty confusing.

So I like Margie's idea of 5(b). I hadn't considered that, but that really gets to my point about the comments. I do like the

"consistent with" or "not incompatible with," but whatever the actual language is within GDPR, I think that's probably the best way to go. Thanks.

JANIS KARKLINS: Okay. Thank you, Mark SV. Volker?

VOLKER GREIMANN: Yes. Two points. First, we can use GDPR language, however, we are not dealing just with GDPR. There's various other legislations around the globe that we also have to take into account. We're just taking GDPR as an example. So it should be consistent and we should, rather than rely on a certain legal framework, rely on the general principles that are outlined.

But back to the original topic at hand, I think the use of the data and the purpose for requesting it is very important for the disclosing entity in determining in their balancing test whether they can disclose that data.

Now, for example if a law enforcement agency comes out and says we want to investigate theft and need to have that data, or fraud and we need to have that data, and that's not a capital punishment issue, then there might be some inclination to give them that data, but if then suddenly they want to use it also to find out who was denying the existence of their particular god, whatever that may be, and that in that country is an offense punishable by death, and suddenly they start to switch around the purpose and want to have other purposes in there as well, then

had we known that before, we certainly wouldn't have given them that data.

So if they actually have to – we have to insist that the purposes that they give us when they request it are the only purposes that they're going to use their data for, otherwise if they can pull a switcharoo after the fact, then the balancing test becomes worthless.

JANIS KARKLINS: I see there's dilemma. The one example that Margie used, I think it's straight forward and could be somehow accommodated in the way that I suggested with the second sentence suggesting that if during the investigation, it appears that the requested data could also be used for another offence, so then there should be some kind of mechanism notification or something to disclosing party that that is the case.

VOLKER GREIMANN: Can I come back on that?

JANIS KARKLINS: Yeah, please.

VOLKER GREIMANN: I think notification isn't going to cut it at that point because you have already handed out that data, and the child has fallen into the well if they started to use it for other reasons, which they obviously can, but then it doesn't carry any penalty.

I think we have to be careful that we do not allow switching of purposes after the request, because the request is what we are balancing the disclosure decision on. If we allow them to change that, then the disclosed decision becomes invalid even if you have a notice in there. I'm not going to have a very happy time if we get a notice that says “Well, we switched the reasons and now we’re going to execute that person, but thank you for the data anyway.” [inaudible].

That’s not going to make my day.

JANIS KARKLINS: I understand that. Okay. Thank you, Volker. Maybe Margie, you can think how to address concerns of Volker. In the meantime, Amr and Mark SV in that order.

AMR ELSADR: Thanks, Janis. I just want to say I completely agree with Volker, and I believe that this proposal of processing the data further for other purposes is not compliant with GDPR, and I'm guessing that the folks who came up with the regulation probably had the same thoughts that Volker just voiced in mind, and also want to point out, which I tried to in the chat earlier, that 5(b) has no bearing on what we’re discussing here at all.

Right now, we’re discussing third-party purposes for processing data, including having the data disclosed to them in the first place for those purposes to process it further. But 5(b) has nothing to do with this at all and cannot be used as an argument or a legal reference for this. 5(b) concerns a controller purpose in collecting

data and ensuring that data is processed – any further processing of this data is done so consistent with the purpose the controller had, not the third party had in collecting the data in the first place. So I just wanted to make sure that we track back this conversation because I feel we're getting a little ahead of ourselves on a false premise. Thanks.

JANIS KARKLINS: Thank you. No, we're trying to explore kind of a real situation that may happen, or may not, but how to reflect that in the policy document. Mark SV, please.

MARK SVANCAREK Hi. I have to disagree with Volker's example because that's clearly a case where the data's being processed in a way that is inconsistent with the request. His switcharoo where I'm looking for data for trademark purposes and now I'm going to execute someone, that's pretty clearly not consistent, so that seems like a false argument there.

If we don't like the 5(b), then we can come up with some other language. I think 5(b) is probably fine. We'll have to look into it. But I go back to my same point, that if we're just making up a bunch of language that's supposed to map to some privacy laws, either existing or proposed, then we're just going to wind up with something that is not really a good fit, so that is concerning to me.

Secondly, I suppose I could put in every request, "I'm looking at this for trademark purposes, copyright purposes and potentially cybersecurity purposes," because all of these things have a

tendency to flow together. Is that what we're really saying? That probably isn't hard to do, but I'm just curious what the purpose of this discussion is, what is the expected outcome of this discussion? And then finally, as another question about the outcome of the discussion, is there – no, I'll drop this last one, so just go ahead.

JANIS KARKLINS: Okay. Thank you, Mark. Now look, I think we are generally in agreement that each request that are put in by a requestor of disclosure of nonpublic data should be unique and should be based on lawful purpose. So that's the premise, and point C with "only" in it tries to clearly state that. So now Margie brought a potential situation that you put forward one request and then it turned out – one purpose, and then during the investigation it turned out that there's a different offence committed by the same person, and how to do it now.

The requestor is already in the possession of data, and then either requestor in possession of data deletes the data and puts a new request or is using the same data that is in the possession but then either do it without any notification or provide some kind of notification to contracted party saying "This is what I discovered, this is what is happening." So this is how I understand what Margie was suggesting or trying to address.

I see Alan's hand is up. Alan?

ALAN GREENBERG: Yeah, thank you. A number of people, both contracted parties and Amr, earlier said that you can't use data that it's incompatible or inconsistent with those purposes. That's the langue that Berry has now, he's using "compatible." "Consistent" I think is a little bit closer, but I'm not sure it makes a big difference.

So I guess I'd like some clarity from people; are they really objecting to those words or are they objecting to something wider than that? because as I said, at least some contracted parties and Amr used those terms earlier. So are they withdrawing that, or are we arguing against something wider than those terms? I'm just not sure. Thank you.

JANIS KARKLINS: Okay. How shall we proceed? Why don't we do it in that way? We will think with staff if there's any other proposal that we can come up for the second reading, and maybe at this point, we move to the next subpoint since time is ticking. Will that be okay? Any objections?

No, I think we're on subpoint D currently on the screen. Must handle data subject personal data in compliance with data protection laws such as GDPR. Alan.

ALAN GREENBERG: My only concern with that is we may end up with data protection laws in different jurisdictions which are inconsistent with each other, and therefore may be in a catch 22 situation by using wording just like this.

JANIS KARKLINS: Do you have any proposal?

ALAN GREENBERG: Maybe data protection laws applicable to the jurisdiction of the data controller and/or the requestor, something like that.

JANIS KARKLINS: Haven't we settled this already last time with applicable data protection laws? Can we say that?

ALAN GREENBERG: I don't remember that, but [inaudible]

JANIS KARKLINS: In compliance with applicable –

ALAN GREENBERG: That would satisfy me.

JANIS KARKLINS: And then take out "Such as GDPR." So, any objections to proposal of subpoint D? I see none, so we moved it up to before C and then left it unchanged at least for the moment. Any other point that need to be raised in this subsection? No, let's then move to subsection ... What was the next building block? H, which pertains to applicable to disclosing entity. Can we get first to the – I

assume that not everyone has read what is in yellow now, and let us take the [first] subpoint.

Subpoint A, and again, with “enforce,” there would be compatibility with the previous building block in [chapeaux] and “enforced by,” that should be understanding.

So subpoint A, must only supply – that is the disclosing entity – the necessary data requested by the requestor. Amr.

AMR ELSADR: Thanks, Janis. This is probably a pointless intervention, but I'm just wondering why we’re using the word “supply” here and not “disclose.” Shouldn’t it read “must only disclose the necessary data requested by the requestor?” I'm just wondering if there was any thought on why supply is [inaudible].

JANIS KARKLINS: No, I don’t think so.

AMR ELSADR: Alright, thanks.

JANIS KARKLINS: Thank you for catching this. No requests? Okay, subpoint B, disclosing entity must return current data in response to request. Kind of statement of obvious. No comments on this point. Disclosing entity must process data in compliance with data protection laws.

Amr's asking, in subpoint B, shouldn't we systemically use "disclose?" No, not there, instead of "return." Thomas?

THOMAS RICKERT: Thanks very much, Janis. I wasn't quick enough raising my hand on point B. I would probably add "Must return" or "Must disclose current data or a subset thereof in response to requests." So I think not all disclosure requests warrant that all the data that is on file has been returned.

JANIS KARKLINS: Could you explain why "Subset thereof?"

THOMAS RICKERT: Let's say there's a trademark infringement and let's say that a [taxi] is provided by the registered name holder. Then in order to pursue the claim to go after the trademark infringer, it's sufficient for the requestor to obtain the data of the registrant and they don't necessarily need the [taxi.]

So in the light of data minimization, we can only craft a policy that allows for the disclosure of data that is actually needed for the purpose in question, and that might only cover a subset of the data that's on file.

JANIS KARKLINS: Okay. Thank you for explanation. I have a few hands now up. Some have disappeared, by the way. I see now Alan and Greg, and Mark, in that order. Alan, please.

ALAN GREENBERG: Thank you. It's more a question. I'm not sure even which item it applies to. At one point, we had a prohibition on requesting nonredacted data, that is you could only request redacted data, not the public data, and there was an argument made that if you did that, you might have raised conditions where you're getting redacted data that was not compatible with the public data at the time the person looked at it just prior to making the request. Did we remove that prohibition, or is that still somewhere there in the background?

I don't know whether we have removed that prohibition [inaudible].

ALAN GREENBERG: Let's just make a note to check, because if we did, then I believe we have a race condition situation which could lead to inappropriate actions, and I'd like to make sure we don't have such a prohibition, but I'm not sure it fits in this particular item or not. Thank you.

JANIS KARKLINS: Thank you. Staff will check on that. Greg.

GREG AARON: Thank you. I think the addition to B is extraneous because A says you're only disclosing the necessary data. B also says it's going to disclose current data. That doesn't say which data or the whole

set or just a little bit. So I would suggest removing “or subset thereof.”

Also, what Alan says is important. We need to come back to that issue and get it settled. SSAC’s strongly in favor of if I request data, I can also get the public set at the same time I'm getting a redacted piece of data. You need to have those at the same time. And it’s also technically trivially easy to provide the public data at the same time you provide one or more pieces of redacted data. Thank you.

JANIS KARKLINS: Okay, thank you, Greg. Marc Anderson.

MARC ANDERSON: Yeah. My comment was on C, are we ready to move to that?

JANIS KARKLINS: No, not yet.

MARC ANDERSON: Okay, I'll put my hand down for now.

JANIS KARKLINS: Okay, thanks. Aiden, yours was also on C?

AYDEN FÉRDELINE: Yes, also on C.

JANIS KARKLINS: No, okay, then let's wait. I have a feeling that the change of disclosure in subpoint A was valid, but when it comes to subpoint B, here we're probably talking about the physical action of return, physical sending. No, sorry, disclosure here is also good.

On the subset thereof, Thomas, would you agree to withdraw your proposal or adding "or subset thereof" following Greg's argument?

THOMAS RICKERT: Strictly from a GDPR language perspective, I think it should be sufficient with the language that we find on the screen without my addition, but I'm just not sure whether the reader understands it that way. I guess that every requestor might think that the data they request is necessary for the respective purposes. So I'm not looking at the necessity from the requestor's impression side, but I'm looking at the data subjects that we sign off on as being necessary for the specific, let's say, use case if we go the use case route.

So as I mentioned in the chat, I'm not concerned about where we put it, but I think it's worthwhile clarifying somewhere that data disclosure requests will not necessarily return the entire set of nonpublic public registration data but only the data that is necessary to fulfill the purpose of the request.

JANIS KARKLINS: Can't we use the same as we're using in subpoint A? if we say disclosure current necessary data in response to request. We're consistent in using "necessary data" not "all requested data."

THOMAS RICKERT: My microphone is conveniently not yet muted again. Would it be okay for you to think about it for a moment and come up with a suggestion on the list?

JANIS KARKLINS: Yes, of course. For the moment, let's put "or subset thereof" in brackets and then see whether that could be somehow accommodated potentially necessary in the same sentence after "current necessary data" but also "necessary" in brackets simply to capture the – no, on subpoint B. "Necessary." There.

So we're now moving to subpoint C, process data in compliance with applicable data protection law. Ayden.

AYDEN FÉRDELINE: Thanks, Janis. Actually, I was going to suggest that data protection law just be changed to applicable law, and perhaps it could be with applicable law including the GDPR and fundamental rights and constitutional protections. But I think it's just making it clearer that it is not just data protection laws that need to ...

JANIS KARKLINS: Yeah, applicable law, the same that we did in the previous.

AYDEN FÉRDELINE: Yeah, the applicable laws, and including the GDPR and fundamental rights and constitutional protections.

JANIS KARKLINS: Aren't we shooting too big bullets? Applicable law and law encompasses constitutional law, privacy law, criminal law, every law. If law is applicable, it's law which is applicable. Would you agree, Ayden? Simply to keep it as simple as we can.

AYDEN FÉRDELINE: Yeah, I don't disagree with what you're saying. It's just a helpful reminder to the reader that there are also fundamental rights and constitutional protections that bear consideration at times.

JANIS KARKLINS: Okay. Thank you. Let's collect other opinions. Margie and then Alan. Margie, please.

MARGIE MILAM: Sure. Thank you. I disagree with Amr's suggestion that we spell out applicable laws. This policy needs to apply globally and we just will not be inclusive enough. So I agree with your suggestion, Janis, to keep it "applicable laws."

JANIS KARKLINS: Okay. Thank you. I don't see that Amr object to that, but maybe it's in the chat. Alan, please.

ALAN GREENBERG: Thank you. I'm a little bit worried we're using slightly different wording in each case. Here we're saying applicable laws. The other case, we say law such as, or privacy laws. I think we need to be consistent in our wording. Thank you.

JANIS KARKLINS: Actually, that is very advisable, to use exactly the same terminology, and we need simply to think whether applicable laws would be used throughout the policy. For the moment, we can also add applicable privacy laws, as we did also in the other building block, which was D. We will fix that with the staff and we will propose for the second reading. Marc Anderson, you had something on subpoint C, I recall.

MARC ANDERSON: I did, but it's been covered.

JANIS KARKLINS: Okay, thank you. Subpoint D. Straightforward. Okay, subpoint E. The disclosing entity where applicable must define and perform a balancing test before processing the data. The data subject should be able to challenge with the proper substantiation the balancing test with the rights to object and to erasure. Alan.

ALAN GREENBERG: Thank you. I'm actually back on D. Do we need to be specific as to whether you're logging the existence of a request, who it was from, what data was provided, and what level of detail do we want to be specific here or do we leave that up to the contracted parties to decide? I don't really care, but I think we need to be careful as to what we're seeing. If we mean one thing, we need to say it.

JANIS KARKLINS: Okay. Thank you. Maybe we can then take E and then return to D talking about your concern, Alan. So any comments on E? Margie.

MARGIE MILAM: In E, it seems like we're confusing two concepts. One is the performance of the balancing test that's required, the other is the challenge. So I would suggest those be separate, and I think we should probably deal with the data subject challenge issues in a separate recommendation. These are all areas we need to obviously talk about and address, but I think that coupling it with this particular supply side doesn't make sense to me. And when we talk about erasure, I don't understand what that means. I'm only suggesting that we do what is required under GDPR and not have a policy that could be interpreted broader than what is required under GPDR. So the right to erasure I don't think is a standalone under GDPR. So I think these are just concepts that need further fleshing out, and I suggest we do it in a separate policy recommendation.

JANIS KARKLINS: Okay. Thank you. So your suggestion is to split this paragraph in two parts. Let's see whether that is something others can accept. Mark SV and then Greg.

MARK SVANCAREK I mostly agree with Margie, I think we should split it into two parts. I don't understand what erasure means in this context. I would point out that – well, I guess it already says "where applicable, perform a balancing test," so no change needed there. Thanks.

JANIS KARKLINS: Okay. Thank you. Greg?

GREG AARON: The second sentence seems to go beyond what GDPR requires. Data subjects need to be told up front about the uses their data may be put to and who it may be disclosed to, but it doesn't give them a veto right, which is what's proposed here. So that second sentence is an overapplication of the law and it's not appropriate to apply to all cases. It might be applicable in a certain type of case under GDPR, but let's also remember that most of the data that's currently redacted from RDS is not covered by GDPR. It's with data subjects and data controllers outside the European Union. So the second sentence doesn't make sense to me at all and we might want to strike it.

JANIS KARKLINS: Okay. Thank you. So for the moment, I would suggest that we put that second sentence in brackets, but we still have a few members in the line. So Ashley and then Volker. Ashley, please go ahead.

ASHLEY HEINEMAN: Hi. Yes. So I have a question with respect to in the first sentence, "must define and perform a balancing test." I'm completely on board with perform a balancing test. I'm just a little concerned about saying here that it is the responsibility of the disclosing party to define it, only because that kind of rules out our ability to, as a community, define a standardized process even if it's at a high level in terms of what a balancing test should look like. So I just wonder if we need to include here this reference to define or just leave it as "Must perform a balancing test" or think of some alternative language that doesn't kind of lock us into a paradigm where if there's multiple deciding parties, that they're defining their own approach each time, which isn't very transparent or predictable. Thanks.

JANIS KARKLINS: Thank you, Ashley. Shall we put "define" in brackets just for memory? Volker, followed by Amr.

VOLKER GREIMANN: Yes, thank you. I think – and I'm not the one who put it there – the right to object and erasure refer to a specific right that the data subject has resulting from the GDPR. The right of erasure seems to refer to the right to be forgotten as in the right of every data subject to have certain data released if there is no further purpose

for it to be process. And the data subject also has the right within the framework of the GDPR to object to certain forms of processing of this data even if it has been legally collected previously. For example, the data subject can say "I no longer agree to the processing of this data, please delete it now," with all the consequences thereof to a domain name registration obviously. However, I think as these refer to certain rights the data subject has under the GDPR, I'm not quite comfortable yet with deleting them at this point. I think this warrants further review and discussion of what is meant by this and what the framework of this right to object and erasure should be, and maybe we can find a way that this is agreeable to all. Let's not move ahead on deleting these right now. Let's think a bit more on this.

JANIS KARKLINS: Yeah. No, Volker, it was Greg who suggested to delete it. I said let's put it in brackets and see what we can do with the text in light of this conversation.

So I have Amr, Ayden and then Greg again, in that order. Amr, please go ahead.

AMR ELSADR: Thanks, Janis. Yeah, I agree with everything Volker said, and I appreciate that we will be revisiting this at a later time. I just wanted to offer my one thought that I put in the chat and just figured I'd say it, and just consider this maybe just as an addendum to what Volker just said, but if a data subject or a registrant during the process of disclosure discovers that some of

its data is incorrect or not current, I see that as one situation where there may be a desire to object to the processing of this data or to have it erased and possibly replaced with more current or accurate data.

So I was just thinking out loud in terms of scenarios where this might be applicable and happy to revisit this at a later time. Thank you.

JANIS KARKLINS: Thank you, Amr. Ayden followed by Greg.

AYDEN FÉRDELINE: Thanks. I wanted to respond to Greg's comments on the second sentence on bullet E. He labeled that sentence essentially a veto right with data subjects. I thought it might just be helpful to clarify that when the right to object under the GDPR is exercised, the data subject must supply a specific reason for why they are objecting to the processing of that data, aside from an objection that was related to direct marketing, and so not all objections will require action, although each must be considered.

So all objections must be assessed and dealt with promptly, but it's not a veto right. there is no guarantee at all about the data subject's request that their right to object is going to be granted. So I think that's an important consideration. Thanks.

JANIS KARKLINS: Thank you, Ayden. Greg and Mark, and then we need to draw the line. Greg, please.

GREG AARON: Thank you. There is a right to object, but it's to sometimes general uses. But every time someone's data is used, we don't go to them to ask if that particular use in that particular case, in that particular instance, is okay.

If you don't want your data to be used or marketing for example, you can go tell people "Stop it," but every time I want to use it for marketing, if I have gotten that right, I can use it and [tell you to tell me to stop.] So there is a difference here that we need to get synchronized on.

Now, the term "where applicable" I suggest be replaced by "where required by law" or whatever formulation we're going to use. "Where applicable" seems pretty squishy. And again, we're interested in compliance with the law but not opportunities to require things above and beyond what is required by the law. Thanks.

JANIS KARKLINS: Thank you, Greg. Mark SV.

MARK SVANCAREK Regarding the concept of a veto, the statement is unclear about when this challenge occurs. If it occurs – for example, in F, if there's a notification to the data subject, somebody's processing

your data. If they are immediately able to challenge that and say, “Hey, don’t process my data in this particular case,” then that basically is a veto because then it interjects some period of delay which may be inappropriate.

If on the other hand the data subject says, “Oh, I realize that you have processed my data and I object to that,” then it would not be a veto. So we should just have some mutual agreement on what this means in this bullet. Thanks.

JANIS KARKLINS: Okay. Thank you. Thomas is the last one.

THOMAS RICKERT: Thanks very much, Janis, and this is a response to Greg. I think we can replace “where applicable” with “in cases of 6.1(f),” because that’s actually where a balancing test needs to be applied, and it can't be more transparent than that.

Just on the mechanics of the objection, it is correct that the opportunity to object needs to be offered whenever a certain processing activity takes place, but we need to make sure that all this information goes into the information that goes to the data subject when in time the data is being collected. And therefore, I think we should keep it in there and the objection may come in at a point in time when the data is requested and we haven't yet decided at which points on an ongoing basis data subjects will be informed about requests for their data.

So I would suggest that we retain that, not make any changes to that, the right to objection as well as other rights in the GDPR need to be made transparent to the data subject. Thank you.

JANIS KARKLINS: Thank you, Thomas. We put the whole subpoint E in square brackets for the moment. Based on this conversation, staff will contemplate and maybe come up with the proposal for the second reading. And let us now visit subpoint D.

So Alan raised the issue, "be more precise and define what type of information should be logged." So, any thoughts on that? Amr.

AMR ELSADR: Thanks, Janis. Just, again, what I said in response to Alan in the chat that I think spelling out what exactly needs to be logged might need to be useful when the policy recommendations are being implemented. So I think it's a thought worth exploring. Thank you.

JANIS KARKLINS: Thank you. Alan?

ALAN GREENBERG: Yeah, just one more thought. Of course, anything we log is subject to GDPR because it probably includes personal information of the requestor and of the data subject, and I guess it's also subject to retention rules and things like that. So we may want to talk about retention in our policy or in our guidance if not in the policy itself. Thank you.

JANIS KARKLINS: One of the building blocks, Alan, is retention and destruction of data, so we'll be talking about those issues there.

ALAN GREENBERG: Sorry, just pointing out that the log itself now is personal data. Thank you.

JANIS KARKLINS: Yeah, thank you. Okay, now for the request, let us move then to subpoint F, disclosing entity must disclose to the registered name holder, data subject, on reasonable request, confirmation of the processing of personal data relating to them per relevant data protection laws such as GDPR.

Mark SV.

MARK SVANCAREK This is a question for Chris. Chris, as law enforcement, what are your expectations about confidentiality of a data request such as this? Thanks.

JANIS KARKLINS: Thank you. Chris, are you ready to respond? Please go ahead.

CHRIS LEWIS-EVANS Yeah, so Chris Lewis-Evans for the record. I think we had it elsewhere that in law enforcement cases, some form of

confidentiality would be required. We have our own processes around disclosure, so I think that would have to be worked out for law enforcement requests. Anywhere that has an impact on an investigation would obviously be detrimental for us, but at the same time, we need to put appropriate safeguards that can be released at an appropriate time.

So yeah, it needs a bit of work about how we tie that into this language.

JANIS KARKLINS: Okay, thank you. My reading of subpoint F is that there should be reasonable request before disclosure to data subject that their personal data has been processing, or my understanding is completely off the target. Mark SV followed by Alan.

MARK SVANCAREK Thank you. Do we need to be more specific about what data is returned to the subject? That is, are we telling them who it was, who asked? I presume we tell them the date and which data elements were asked for, but the question of, are we specific [about] who the requestor was? Okay, that's an open question. Marc Anderson.

MARC ANDERSON. Thanks, Janis. Another follow-up question for Chris. Again, more on the topic of confidentiality. I certainly understand there are cases where confidentiality isn't just desirable, it's necessary. In those cases, would you envision working through the SSAD

system, or would you consider that sort of a separate process where you'd go directly to the data controllers?

I guess my question is, how much do we need to account for confidentiality in defining building blocks for the SSAD? If it's necessary, let's do it, absolutely, but I'm wondering if that's really a use case for the SSAD system or if that would be more something for one-off processing.

JANIS KARKLINS: Okay, thank you, Marc, for question. While Chris is thinking, Georgios is speaking.

GEORGIOS TSELENTIS: Yes. practically, we have here the F and G which are dealing with the same problem. We are talking about whether the registrant has the right to find out whether his personal data are processed, and with GDPR saying that if they're under investigation, there should be a level of confidentiality. There is another factor which is the factor of time. So definitely, I think if there are investigations, we said I think somewhere that they need to be logged, so we cannot investigate things without having this type of activity not monitored and logged, but at the same time, if the disclosure can happen after the investigation is performed, I don't know if this solves the problem or creates another one. So in other words, there is an issue of timing, of when the disclosure of the investigation is happening, it can happen a posteriori. I don't know if F is respected in this case, and then G does not – so the law enforcement does not abuse their right to make the investigation.

So that's what I wanted to stay, that there is an issue of timing of those two activities, when the subject can request, whether its personal data are being processed, and whether an investigator can continue to conduct the investigation without revealing the investigation to the data subject, for obvious reasons. Thanks.

JANIS KARKLINS: Thank you, Georgios. Chris Lewis-Evans.

CHRIS LEWIS-EVANS Thanks, Janis. Just to quickly answer Marc's question, realistically, we have to satisfy our own internal requirements for doing a request, our purposes for the investigation of crime. So realistically, every single request would have some form of confidentiality. Certainly, at my level which is a national level. As you get lower, that might be less. If you're looking at something a little bit less serious – but realistically, I would say – and don't quote me on this, obviously – two thirds plus of requests would require some form of confidentiality. And as Georgios says, that's not confidentiality forever, that is based on the time basis for the investigation.

JANIS KARKLINS: Chris, you know that you're on public record now, we will quote you anyway. I'm just joking.

CHRIS LEWIS-EVANS Yeah, I know. That's why I love being on this EPDP.

JANIS KARKLINS: Okay, thanks for your comment. Ayden followed by Volker, and then we need to wrap up this part of the conversation.

AYDEN FÉRDELINE: Thanks, Janis. Just responding to the question that Alan Greenberg put out there a few moments ago, Alan asked for clarity over what information would be provided to the data subject, should they make a request, and I know that we don't want to rely solely on the GDPR here, but I think that the GDPR can help us in answering part of his question. Article 15.1(c) of the GDPR says that any third parties to whom data has been disclosed must be named. And if we also turn to some advice from Article 29 data protection work party, which I've put in the chat there, they have said that third parties to whom data has been disclosed must be named with contact details, and they have said that by default, controller should name the recipients and not categories of recipients, and that if they choose to name categories instead, this can only be justified in exceptional circumstances and they must justify why this is fair.

So I think that is helpful, that when we're thinking about, should a registered name holder submit such a request, they should reasonably be informed with the names of precisely who has access to their data. Thanks.

JANIS KARKLINS: Thank you, Ayden. Volker?

VOLKER GREIMANN: Yes, just one point. With regard to the legal investigations, most law enforcement officers of competent jurisdiction at least have the power to compel the party they're requesting a disclosure from not to disclose that fact because it's essentially for the ongoing investigation. And I'm happy to put in a disclaimer or side note to that effect, that obviously, in case there is a valid – that the disclosing entity is compelled by the requesting party with a valid request not to disclose that fact of disclosure in that case, disclosure to the data subject may be foregone or postponed until the reason for nondisclosure is over.

So whatever the case may be, I think there are reasons where law enforcement can request that they have the legal right to do that, and in that case, obviously the rights to disclose prior to disclosure would not be applicable. So I would be happy to see language added to that effect.

JANIS KARKLINS: Okay. Thank you, Volker. We'll think about it. Mark SV is the last one on this topic.

MARK SVANCAREK Thanks for squeezing me in at the end. I think a lot of our conversation that we've just had really hinges on the clause on reasonable request. So I think we need to think about where that phrase "unreasonable request" is controlled within law or work party 29 guidance in order for this to be effective and avoid downstream arguments. Thanks.

JANIS KARKLINS: Thanks. Look, I think we have now enough material for staff to relisten and then rethink, and modify certain sections of this building block that we can then revisit them during the second reading.

Alex, you have a burning desire to speak?

ALEX DEACON: I'm not too sure I ever have a burning desire to speak, but if we're moving on from this building block, I just wanted to note our suggestion of a new item here, item H that we provided in our comments, the "must provide nonpersonal nonpublic data for data subjects that are legal persons or otherwise not subject to data protection laws."

I think the description at the L.A. meeting from Allan Woods about how he does the balancing test kind of made it clear that for the most part – I think 90% of his cases, 80% of his cases, he can determine that either a privacy proxy is in use or that the data subject in fact doesn't fall underneath the GDPR for his jurisdiction. So I think clarifying and adding a requirement such as we suggest in H would be very helpful. Thanks.

JANIS KARKLINS: Thank you. Can we highlight H? This is in the box, fourth bullet. You see it on the screen, fourth bullet, considering adding H and must provide nonpersonal nonpublic data for data subjects that

are legal persons or otherwise not subject to data protection laws. Any reaction to this proposal? Ayden?

AYDEN FÉRDELINE: Thanks. I disagree with the inclusion of point H because some legal entities, religious entities for instance, are entitled to protections under constitutional law, so I think this language would be very problematic if we were to include it. Thanks.

JANIS KARKLINS: Okay. Thank you for your feedback. Amr?

AMR ELSADR: Thanks, Janis. I'd like to just take some time to think a little more about what Alex is proposing here. I realize that when the EPDP team recommended that there should be no differentiation or differentiation should not be required of contracted parties in terms of legal and natural persons, that was on whether the data was redacted to begin with. It's not an issue of disclosure. So I don't want to necessarily tie the two together. But I just would like to think about a little more about what it would mean to add the word "must" in H here. Thanks.

JANIS KARKLINS: Okay. Alan Greenberg.

ALAN GREENBERG: Thank you. We were told way back, early in the process, one of the first meetings, that there are laws that identify entities that are legal entities but still eligible for privacy. And religious organizations may be one of them. There may be others. But we were told that in some national laws, there are carveouts. So I'm fine with putting carveouts here, but I'm not fine with eliminating the concept in general. Thank you. So I'm supporting H with carveouts if necessary to cover the kind of cases that Ayden was referring to. Thank you.

JANIS KARKLINS: Okay. Thank you. Marc Anderson.

MARC ANDERSON: Thanks, Janis. I'm a little uncomfortable with H as it's written as well, sort of echoing what Ayden said. I'm concerned that here may be some unintended consequences with the language the way that it's written. I understand what Alex is going for, and certainly, to his point about Allan Woods' presentation on his path to making a determination on disclosure of data, certainly if there's a clear determination that there's not personal data subject to applicable data privacy laws, then there could be a decision to disclose. But I think that the language, H, [S,] as Alex has written, does not appropriately take into account all the nuances here.

So I guess what I'm trying to say is I'm sympathetic to what Alex is going for, but maybe not his proposed language, if that makes sense.

JANIS KARKLINS: Okay. Thank you. And Volker is last. Volker, please.

VOLKER GREIMANN: Yes. I'm also uncomfortable with language because of the main fact that this language, again, seems to indicate that legal persons are not subject to data protection laws, or at least the data of legal persons is not subject to data protection laws. This is incorrect. Legal persons' data may still contain personal data of natural persons, therefore the data that is contained in the data of legal persons may still be protected and therefore the formulation of this is absolutely incorrect and would have to be changed significantly to reflect that fact.

I think we've discussed this before. I don't need to go deeper into this now.

JANIS KARKLINS: Okay, so thank you. Maybe if I may suggest that those who have proposals to how this H could be reformulated, please add either drop now them in the chat box as we continue speaking or send them to staff that they can contemplate and propose maybe for the second reading. For the moment, maybe we need to capture the concept itself, but with understanding that the current language would not stand fully the ground.

So with that, can we move on to the next agenda item that we still have to examine? Time is really short. So with your permission, let us talk a little bit about the receipt of acknowledgement. So there was already considerable traffic before the meeting. Ayden proposed a new wording which was discussed by other team

members. For the moment, I understand that Ayden's proposal is not holding ground in terms of consensus, but let me open the floor and see maybe gather the general comments on this, which to me seems rather technical question.

So the staff proposal is on the screen, and Ayden's proposal was sent in e-mail a few days ago and triggered e-mail traffic on that . So, who will start? Ayden suggests that he will paste his proposal in chat room as we speak. Amr.

AMR ELSADR: Thanks, Janis. I'd just like to ask for clarification on the lack of consensus for Ayden's proposal, because I think there are multiple parts to the proposal. One was to provide the data subject or the registrant with a notice that a disclosure request has been submitted for its data. The other part was an opportunity for data requestors, affording them to perhaps amend their data request or maybe correct information that is not accurate.

The sense I got from Greg's response at least is that this would unnecessarily prolong the process in which the data requestor would receive data. So I'd just like to be clear if there was objections on one or both parts of Ayden's proposal.

Speaking for myself, I think the notice to the registrant that a data disclosure request has been submitted, I think that's a reasonable addition to this building block, and I'm assuming that this is something that could be automated somehow and would not require terrible burdensome overhead in terms of what contracted parties might need to do. But this is all just a question. I'm just

thinking out loud. So the more information I have from the review team members on this, the more helpful that would be. Thank you.

JANIS KARKLINS: Thank you, Amr. The text which is now on the screen comes from the phase one report recommendation 18, it [is at the] very bottom. And I think that here, we have two different things. One thing is to acknowledge receipt of the request that should go to requestor. So that would be one action. The second is the information about that request has been submitted that needs to be sent to data subject. that is different, and I'm not sure whether that would fall under the title receipt of acknowledgement.

Alex, are you in agreement with me?

ALEX DEACON: Janis, hi. Yes, actually, I am in agreement with you. I think that for the purposes of I guess the work that we need to do, this building block should focus on the receipt of acknowledgement in response to a request. We can talk about side effects of submitting requests to the data subject somewhere else. So I agree with you on that.

In terms of the specifics of receipt of acknowledgement, as I mentioned on the mailing list and as I mentioned also in my comments on the zero draft or the draft zero, assuming a future implementation of an SSAD that uses what I called modern web services technologies and frameworks, so things like RDAP and the technology that the TSG suggests can be used for authentication and authorization.

So we're not talking about letters and other old-fashioned technologies here. It's pretty clear to me that when those technologies are used, an acknowledgement of the receipt of the request needs to be instantaneous. We're no longer talking about a phase one recommendation 18 scenario here where e-mail may be used and people are out for the weekend and for bank holidays and the like.

We're talking about a system, a web service, if you will, that is up and running 24 hours a day under some TBD SLAs, and thus when a request is sent, an acknowledgement that the request has been received should and can happen instantaneously. It does not mean, for the avoidance of doubt, that we're expecting or anyone should expect nonpublic data to be returned, but at a minimum, a response that says, "Thanks, we've received your request and we're working on it" or there's an error with it or some other appropriate response should be returned instantaneously.

So that was kind of the point of my question to Ayden and my point here for building block K which is, let's focus on the receipt of acknowledgement and ensuring that that happens instantaneously or as quick as possible. We're talking about milliseconds here. Thanks.

JANIS KARKLINS: Yeah, thank you. Let me take Alan Greenberg now.

ALAN GREENBERG: Yeah, thank you. My comment is essentially similar to Alex's. If I fill out any webform and I don't almost instantaneously get a

confirmation that it has been received, it's a very broken website or very rude people. So that part should be a given.

Now, whether it is specific in saying I've analyzed it and you've omitted a part of it, or not, that's a different issue. But an acknowledgement should be virtually instantaneous no matter whether we have a centralized system or not. Thank you.

JANIS KARKLINS: Thank you. Ayden, in light of what you heard now, would you agree that your proposal, specifically that part that relates to informing data subject, that request has been filed would be dealt elsewhere, not in this building block.

AYDEN FÉRDELINE: Hi, Janis. Yes, I think that is fair to separate the two. So yes, I would agree that. The second component of the text that I proposed, which was essentially rights for the registrant, that could fit into another building block perhaps. So yes. But I do think that there is value in the first part of the text that I proposed, and that is spelling out precisely what the receipt acknowledgement letter would contain.

And just to clarify, the proposal was never for there to be a physical letter to be sent to someone. Of course it would be electronic. What I was trying to do was to look at how things happen in other areas. And in freedom of information access law, it is well established what these letters contain, timelines, processing conditions, and the rights of the requestor.

So this was really just trying to sort of set out that this is not a one-way street here and that the requestors of data have some rights as well, as well as responsibilities, and that they should be able to make minor corrections if there is a typo in their submission or the wrong contact details are provided, and that they should not have to start the process all over again by submitting a new request, which would potentially delay them even further.

And it was also taking into consideration that we don't know what the system will look like. It could be quite decentralized. There could be a human review process in the end. So the time to actually allocate this request to a human to review it may not be instantaneous. So what this receipt acknowledgement letter would ideally do would be providing a point of contact for the requestor as well so that they have a human that they're able to contact with request to follow up on their request. Thanks.

JANIS KARKLINS: Thank you, Ayden. It's clear. Thank you for clarifying this. I think in Los Angeles, we agreed that whatever system we're building, that should be as much automated as possible, and otherwise standardized.

So to my limited knowledge of technology, [I was brought up on lamps as a radar engineer,] so I understand that at least requesting side could be automated no matter who is filing this request, whether that is accredited entity or individual from the middle of nowhere. And that would be web based with immediate return if the field is either not properly filed or contains some errors. So thank you for your comment. That, we need to factor in.

How the request would be processed is a different story, whether that would be automated or manually processed. That should not prevent sending immediately a receipt of acknowledgement saying, yes, your request has been received.

Okay, and then we would talk about notification of data subject in other place and in other building block. In that understanding, can we hope that staff would reword the proposed receipt of acknowledgement building block and present it for the second reading, for the team? Good, I don't see any requests for the floor.

So then I would suggest that we go to the next agenda item of today's meeting, and that is, who should be responsible for disclosure decision. Look, we do not have much time, but if I may ask Caitlin where we are now with the additional inputs, could you tell who provided those inputs?

CAITLIN TUBERGEN: Hi, Janis. Yes, and I see that we have additions from ALAC, and it looks like we just received an addition from GAC colleagues as well. I don't know if we want to ask those groups to briefly present on their ideas or if you'd like to wait for more comprehensive responses from the other groups before we get into that.

JANIS KARKLINS: We do not have much time on this, but would it be possible for ALAC and then GAC in three minutes simply to tell your narrative, your vision, how you see that? I see Alan's hand is up. Alan, please, three minutes, not more.

ALAN GREENBERG: Thank you. I'll be less than three minutes. the gist of our point is that we don't believe that a single size will fit all. We believe that there should be some classes of requests that are handled instantaneously and by a centralized authority. It doesn't much matter whether it's ICANN or this trust that we're talking about, although we have some lack of understanding at the trust based on the presentation that was made in L.A.

But we believe that there are some levels of requests which are almost always going to go back to the registrar by they will need some level of specific analysis and balancing. But there should be some types of requests, and we give several examples in our submission that we think can be automated and can be done at a level by ICANN Org or whoever, however we set up some centralized thing.

So the bottom line is we don't believe there's a single answer, and the system should have some flexibility based on a number of parameters. Thank you.

JANIS KARKLINS: Okay. Thank you, Alan. Ashley.

ASHLEY HEINEMAN: Thanks. We kind of tackled this, recognizing that this doesn't include everything but just kind of at a high level adding points that aren't necessarily reflected already, which for both – I guess first off, we did not comment on the data trust concept because we felt

that there were too many variables that were unknown, so we limited our comments to basically contracted parties and ICANN Org.

So for both, we believe there need to be legal agreements in place between ICANN and the contracted parties that clearly articulate the roles, responsibilities and the corresponding recognition of risk associated. We believe that there needs to be a strict and timely time frame by which there will be a confirmation of receipt of the request, as well as for making a determination for disclosure. And this would all be dependent on the purpose.

We think in both cases that there needs to be a community agreed upon standard for conducting a balancing test to ensure as much predictability and transparency as possible, and that there be a strict corresponding monitoring and enforcement regime.

The only real difference here is that under the ICANN model, we think that there needs to be a clearly articulated recognition by ICANN on its roles, responsibilities and acceptance of the corresponding risk. That seems to be the biggest roadblock in terms of proceeding with this kind of centralized approach.

So that's it in a nutshell. Thanks.

JANIS KARKLINS: Thank you. Caitlin, who hasn't filed yet the comments?

CAITLIN TUBERGEN: Thank you, Janis. We're still waiting for comments from the Business Constituency, the ISPCP, the NCSG, the RySG and the SSAC.

JANIS KARKLINS: Okay. May I ask those groups to file as soon as is feasible? That would be very helpful for our consideration. And we will monitor situation and see when responses come in. We'll provide as snow the opportunity to comment briefly conceptually the vision, and once everyone will have this information in, then we will do analysis and see where we are with this. Probably the most important topic that we need to agree upon.

So with this, I would like to bring this meeting to closure unless there is anyone wishing to speak on Any Other Business. If not, then thank you very much for your active participation. We are meeting now on Thursday which is in two days. The proposed agenda will go out as soon as this meeting is over, and we're looking forward to have conversation on suggested agenda items on Tuesday.

With this, thank you very much for participation in this meeting, and I wish you good rest of the day. This meeting is adjourned.

TERRI AGNEW: And once again, thank you everyone for joining. Please remember to disconnect all remaining lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]