ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Thursday, 30 April 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/1iqJBw
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 30th of April 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 Amr Elsadr, NCSG, James Bladel, RrSG. They have formally assigned Owen Smigelski as the alternate for this call and any remaining days of absence. All members and alternates will be promoted to panelists for today's call. 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. 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.

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 55th call of the team. Agenda is in front of us and first question as usual, can we follow this proposed agenda? I see no hands raised. I take that

this is acceptable, and we're moving to the first substantive item of the agenda. It is housekeeping issues. On Tuesday, there was a meeting of legal committee and I would like to ask Becky to brief on the outcome of the work of legal committee. Becky, over to you.

BECKY BURR: Thank you, Janis. We received a memo from Bird & Bird on the automation use cases. The memo has a very good executive summary which we commend to you. As you will recall, we gave them two scenarios. The first one would be where the central gateway made an automated recommendation to the contracted parties which the relevant contracted party could accept or reject, and in scenario two, the decision to disclose would actually be taken by the central gateway rather than the contracted parties.

Bird & Bird went through the provisions of article 22 of GDPR, which pertain to automated decisions, and essentially reminds us that solely automated decisions can only take place where—the GDPR doesn't apply because there's no personal data, or the decision does not have legal or similarly significant effect on the data subject. There are some member state [delegations] and authorizations which they point to that may apply in particular EU member states but they're not inform or uniformly available to ICANN.

There were a series of questions that we were posed and I will tell you that some general conclusions that they made that no matter what, even if the central gateway is not reviewing actual registrant data, in their view, a decision to disclose information by the central

gateway would likely invite the processing of personal information such that GDPR and article 22 would apply.

Scenario 1A, which is an automated recommendation that a contracted party followed by an individual review by the contracted party does not rise to the level of solely automated processing. Outside of that context, the 1A recommendation context, the question is really whether the processing and making a decision with legal or similarly significant effects.

They provided a very useful chart that is up on the screen here, and as you can see, they have concluded that there are four situations in which in their view, the decision making does not involve a legally or similarly significant effect. So by a data protection authority investigating a data infringement, effecting the registrant themselves, where the request is for a city field, only to evaluate whether or not to pursue a claim, for statistical and research purposes, if there's no registration data in the record at all, which is obvious but GDPR doesn't apply.

Then they have a couple where they clearly say, yes, this decision to turn over would have a legally or similarly significant effect. For example, if you're turning over registrant data to law enforcement or a data protection authority in the same jurisdiction as the contracted party, then in their view, the purpose of crime prevention, detection and prosecution would be legally significant.

There are a couple of others here, investigation of data protection against—committed by the registrant, exercise of a trademark claim, the decision to exercise a trademark claim, and the decision to share data with a law enforcement and take legal action.

And then the bulk of the use cases presented, they said, well, it's really not clear, and they recommended a series of steps that might be taken, a series of safeguards that might be taken to reduce uncertainty, which included on the one hand a discussion with data protection authorities or the European Data Protection Board, and I think most relevant to us, much better scoping about each use case and its legal basis.

They were asked to talk about the concept of proximate cause with respect to legal or similarly significant decision making. In other words, is there an argument that the decision to disclose registrant data is merely preparatory and therefore not the proximate cause of a decision involving legal or similarly significant effect?

They did identify some literature in some analysis in German legal literature discussing this, and generally supportive of the notion, but it is not case law and it is not generalized across the European Union member states. So I think they suggested that further work—not further work would need to be done but that it was very difficult to know how data protection authorities would come out on that. it's very hard to know where the GDPR falls on that.

They were also asked about the relationship between contracted parties and the central gateway, and so under scenario one, where the contracted party would receive the recommendation but the contracted party from the gateway but would make their ultimate decision themselves, their conclusion was that the parties would be considered joint controllers.

And under scenario two where the central gateway actually made the decision, Bird & Bird talked about two different approaches to this. One is a macro approach where both the ICANN or the central gateway and the contracted parties are involved in the decision-making and therefore the most natural conclusion in this looking at the big picture would be that they're joint controllers. And then they also talked about a different approach that the European Court of Justice has taken in at least one case where the decision with respect to controllership is done on a much more micro basis. So here it's possible there's a reasonable argument—and in fact, I think they sort of liked this argument ,that the contracted party would be controller with respect to the decision to transfer data to the central gateway but where they had no role in the final decision to release it. you could argue that the central gateway was the controller.

Again, this is an argument, it's not—I don't think that they came down—well, I think Bird & Bird thinks that that's a better argument but it is not at all free of doubt for them. and then finally, with respect to contracted party liability, Bird & Bird said first of all that where there's a joint controller relationship, it's important to make sure to allocate the tasks and responsibilities through an agreement, that the contracted parties could only avoid joint and several liability to individuals by demonstrating that they were not in any way involved in the events giving rise to the damage. Situation is a little bit more complicated with respect to liability to data protection authorities.

And then they were asked, as between scenario one where the central gateway provides a recommendation and the contracted

party [inaudible] and scenario two where the central gateway actually makes the decision as between these two which one of those is likely to result in a lower risk of liability. And they concluded that scenario two where the central gateway makes the disclosure decision gives the contracted parties a relatively better argument regarding the no involvement and therefore potentially a lower degree of responsibility for the decision. But just to be clear, this goes back to the argument that they have to demonstrate that they weren't involved in the event giving rise to the damage.

So with respect to the legal committee's discussion on this, we've asked ICANN Org to develop proposals for ways to take the use cases identified by Bird & Bird as not rising to the level of legal or similarly significant event and therefore able to be automated, asked them to develop ways in which those use cases could be automated. And then we also want to commend the use cases identified by Bird & Bird as unclear, perhaps to the small group working on automation issues, along with Bird & Bird's suggested safeguards for making the use cases much more clearly defined and identifying the legal basis in order to see if there's more clarity is available with respect to the legally significant effect.

There's some things about this decision, I think, that people feel differently about, so I do want to give other members of the legal committee opportunity to share their views on this if that's all right with you, Janis.

JANIS KARKLINS: Thank you, Becky. Yeah, let me see if there's anyone from legal committee who would like to come in at this stage with further

comments. I see no hands up. Then next question is, is there anyone from the team who would like to ask questions to Becky or legal committee in general in relation to this presentation and action point? I see none.

BECKY BURR: Okay, probably—

JANIS KARKLINS: It's overwhelming, Becky.

BECKY BURR: Talked everybody to death. Yeah.

JANIS KARKLINS: It's overwhelming, as I told during the legal committee meeting. But of course, I'm looking at next practical steps, and as Becky, you said, we asked ICANN Org, asked staff based on this Bird & Bird recommendation as well as comments that have been provided during the comment period to work on the recommendation in relation to automation and we will examine that draft recommendation at the time when we will be looking at it, hopefully during our next meeting of 7th of May. So thank you very much, Becky, and thank you, legal committee, for discussing and also giving practical guidance to the staff.

So with this, we can move to the next agenda item, and that is a continuation of examination of recommendation eight on response requirements, and just as a reminder, we made significant

progress during the last call but we had not exhausted all issues and there's one remaining on urgent requests.

So since there have been some developments and exchange of views in-between these two meetings, maybe it would be wise to ask Caitlin who is following up this topic to brief us where we are and what would be potential way forward. Caitlin.

CAITLIN TUBERGEN: Thank you, Janis. As you noted, there has been some discussion. Most of you likely saw this on the list yesterday between Mark SV and Volker. But there were some public comments received about the definition of urgent request, so we wanted to remind everyone [on the] message during this exchange that with respect to urgent requests, only accredited entities would be able to make urgent requests and in the event that a contracted party receives an urgent request and believes that it doesn't meet the criteria, it has the ability to demote that request, either a priority two or three depending on the situation.

The current definition that we have includes limited circumstances in which it can be applied, imminent threat to life, serious bodily injury, critical infrastructure, online or offline child exploitation. And I wanted to note that in the message that we sent yesterday, we were wondering if it was worth focusing on a set of examples for these limited circumstances, and I noted that Mark SV came up with some examples which you can see Berry is highlighting on the screen, and we wanted to pose a question to the group: are these examples helpful, acceptable, or are there additional examples that we could give?

We might not get into a detailed discussion about all the potential examples but we thought it might be helpful to get an initial reaction to this since there does seem to be some disagreement about the definition of urgent request and we're looking for a way to move forward here.

JANIS KARKLINS: Okay. Thank you, Caitlin. So idea would be to put those examples in implementation guidance that provide certain idea what these requests or what could be considered as an urgent request outside those that have already been outlined in the text of recommendation.

So any reaction to that proposed way forward? Team members, are you there? Or everyone is in agreement with the proposal?

UNIDENTIFIED MALE: Still thinking.

JANIS KARKLINS: Volker. Chris.

CHRIS LEWIS-EVANS: Thank you, Janis. Happy with the way forward, not necessarily happy with the examples, I think [inaudible]

JANIS KARKLINS: Could you speak slightly louder please?

CHRIS LEWIS-EVANS: Yes. Sorry. So, happy with the way forward but not necessarily happy with the examples, but happy to work on that on the e-mail list.

JANIS KARKLINS: You mean the examples in recommendation subpoint F which is now outlined, or the one that Mark SV has put forward outside those that have been—

CHRIS LEWIS-EVANS: The ones that Mark has put forward.

JANIS KARKLINS: Okay. That would be for implementation guidance rather than for the recommendation itself.

CHRIS LEWIS-EVANS: Yeah.

JANIS KARKLINS: Okay. Certainly, so this is not really critical. Implementation guidance is more information and certainly we need to agree on that, but still, there is a possibility of working on that after we closed the recommendation itself. Volker, your microphone is up. Not hand.

VOLKER GREIMANN: Yeah, just ignore that.

JANIS KARKLINS: Okay. So, no request for the floor. May I take that this would be the way forward? So then there would be separate recommendation on urgent requests which is based on what we see now on point F and G, and there will be examples provided in implementation guidance for those that are not related directly to threat of life and serious bodily injury, critical infrastructure, online, offline child exploitation.

Okay. Good. So I think we have exhausted recommendation eight unless you have any comments on implementation guidance which is for the recommendation eight. So, thank you. Let's move now to recommendation 11.

Recommendation 11 is on disclosure requirements, and as it is usual practice, may I ask Caitlin to give us a general overview? And then go to the first two points related to the heading of the recommendation. Caitlin, please.

CAITLIN TUBERGEN: Thank you, Janis. One overarching reminder with this recommendation 11 for disclosure requirements is that this recommendation is not about who makes the decision but rather what rules apply once the decision to disclose was made. So there was some confusion about that in the comments, just wanted to make that clear so we could focus the discussion.

So Berry, if you could scroll down for the first two questions. The first question about the introduction paragraph talks about or asks if all parties to the SSAD must comply with disclosure requirements if approved for automated disclosure. I wanted to highlight that as an ICANN Org clarification question. And then also related is, should it be clarified who can trigger the enforcement mechanism and what the enforcement mechanism should look like, or is this an implementation question?

And we may need to revisit this question at the end of the discussion of the recommendation to see if based on the discussion, there's a need to specifically differentiate disclosure requirements for automated and non-automated responses.

JANIS KARKLINS: Okay. Thank you, Caitlin. So in all honesty, I personally do not understand the question itself, but maybe I am—if I may ask ICANN Org liaisons to clarify what is unclear and what is a concern.

ELEEZA AGOPIAN: Hi Janis. I can explain it. I had to refresh my memory about the question. I think in looking at the first paragraph of recommendation 11, what we're trying to understand is the [last clause of] that first sentence references as well as any automated responses provided by SSAD. We just wanted to confirm that the requirements recommended here also apply to automated decision making, in other words compels the contracted party to disclose.

JANIS KARKLINS: Okay. Thank you. Alan G, your hand is up.

ALAN GREENBERG: Thank you very much. I don't have an answer to the question, but I have a real problem with the use of the word "automated responses provided by the SSAD." We have periodically talked about the concept that the SSAD may actually have people associated with it helping to make the decision, and therefore a decision from the SSAD is not necessarily an automated decision. And I really think we need to separate the concepts. Decisions made by the SSAD may be automated—if we can figure out how to make that work. On the other hand, there may be staff associated with the SSAD that are helping to make these decisions or making these decisions. So I think we really must separate the term "automated" from "decisions made by the SSAD." Thank you.

JANIS KARKLINS: Thank you, Alan. I think that it is understood that contracted parties would make decisions in not automated way, and if there would be any automation, that would be done at the central gateway level without involvement of contracted parties and without involvement of humans. So therefore, that distinction is already kind of obvious, at least for me.

ALAN GREENBERG: Sorry, if I may have a follow on, decisions by a contracted party could be automated if the contracted party decides that's a legal and safe way to do it. That's completely separate. But we have talked periodically about the concept that the SSAD may have people associated with it and decisions made or recommendations for that matter made by the SSAD may be made not necessarily in a fully automated way. And I don't think we should merge the ideas, because we're ruling out a potential for making centralized decisions that are not automated, and I think that's a possibility that we may end up going to. Thank you. Especially given that we have a lot of small contracted parties that may not be in a position to do this.

JANIS KARKLINS: Okay. I would like to see other views on this, because my recollection is that this understanding was that automation would be done at the central gateway level without human involvement. I do not recall that we talked about the centralized decision making which would involve humans which potentially is UAM model, or at least variation of it. But I may be mistaken. Stephanie, please.

STEPHANIE PERRIN: Thank you. I would just like to point out that this whole issue of intervention in a decision made by the SSAD comes back to this problem that we have been discussing, namely the controllership or co-controllership of the SSAD. If indeed the registrars control that decision, then they are the controllers of the SSAD. So your decision making remains at the registrar level.

If on the other hand ICANN is the controller in this situation, then you get into a separate decision potentially as Alan Greenberg correctly describes, being made at the SSAD level rather than at the co-controllers level. And that's something that I think is potentially—we haven't ruled it out because we haven't dealt with this whole co-controller and division of liability and decision-making power issue, at least to my satisfaction. Thank you.

JANIS KARKLINS: Thank you, Stephanie. We put in the initial report that the working assumption for SSAD was that it's a situation of joint controllership and that is in the initial report as one of the overarching principles.

STEPHANIE PERRIN: If I may be permitted to follow up, but we haven't sorted out that joint controllership.

JANIS KARKLINS: Okay. Any other interventions on this side, on these questions? So I do not have much to conclude on these two points without further input from the team. Marc Anderson, please.

MARC ANDERSON: Thanks, Janis. Let me take a crack at this. Looking at question one, does this mean that all parties to the SSAD must comply with disclosure requirements if approved for automated disclosure? And the disclosure requirements we're talking about are A through

J here. For example, the first one, must only disclose the data requested by the requestor.

So if we're looking at the actual question—sorry, I'm flipping [back], does this mean all parties to the SSAD must comply with the disclosure requirements if approved for automated disclosure? I think the answer is yes. All parties must only disclose the data requested by the requestor. I think if we look through this list, the answer to that question is yes. so if we're tying it back to this question raised by staff, as I read it, I think our answer to this question is yes.

JANIS KARKLINS: Thank you. Brian.

BRIAN KING: Thanks, Janis. I agree with Marc. Thanks.

JANIS KARKLINS: Thank you. Hadia.

HADIA ELMINIAWI: Thank you, Janis. I was thinking also in the way Marc was thinking. So I'm looking at what they need to do. Contracted parties and SSAD must only disclose data requested by the requestor. That's a yes. and B is a yes. Must process data in compliance with applicable law. It's a yes. Must log requests. It's a yes. But when we come to E for example, "Where required by applicable law, must perform a balancing test before processing

the data," if we are talking here about an automated decision, the central gateway already made the decision whether to disclose or not, and if the decision is yes, there's no room here for the contracted parties to look for a balancing test or verify if one is required or not, and accordingly decide what to do.

So I'm not sure that in case of automated requests, the same dataset or the same exact requirements would apply for the contracted parties or the relevant parties. Thank you.

JANIS KARKLINS: Okay. Thank you. Sometimes I wonder whether machines or algorithms rather could not do balancing test in the same way as humans would do because human mind also follows certain logic, same logic could be built into the algorithm. And answering question of Milton that was at the beginning of the session, what purpose of recommendation, that is to develop algorithm and gradually train this algorithm to make these decisions hoping that the recommendation would match the disclosure decision close to 100% at one point in time. Not at the beginning, of course, but at one point in time.

So I have further requests for the floor. Now it's too many. But nevertheless, I have Alan G, Volker and Mark SV in that order.

ALAN GREENBERG: Thank you. On the substance of this question, I think the problem is that some of these "musts" may conflict with each other. When we talked about this earlier, I think James was the one who said, are you really putting a gun to the contracted parties' heads and

saying you must disclose something if they feel it's inappropriate? And my response anyway—and I think others—was there might be extenuating circumstances where a contracted party believes this really contravenes the law and does not comply with the disclosure, and of course, should Compliance question it, they would have specific reasons why, there were extenuating circumstances and they did not comply. They can't just whimsically not comply, but there may be circumstances where they feel that the applicable law in fact says they can't even though the automated decision was made. And I think we have to give contracted parties that out unless joint controller agreements really ensure that they're being free of any liability of doing it. So, thank you.

JANIS KARKLINS: Thank you, Alan. Volker.

VOLKER GREIMANN: Yeah. I'm not sure if I'm maybe reading this wrong, but approved for automation might mean a variety of things. We had already agreed that the SSAD might allow contracted parties to flag certain things for automation on voluntary basis, and that would certainly also fall under the category, but making that a requirement at this stage would probably not be wise or even sensible thing since we're disclosing voluntarily.

To what Alan just said, if it's automated, then there is no more human review, so if we feel that it is illegal to process something, then we're still out of luck because the automated process will

have already gone through by the time that we know that it has gone through, so that is not the solution either.

But finally, to what Janis said, if we ever find that magic algorithm, I'd be the first one to use it, but I still feel that artificial intelligence is not quite there yet where it can make sense of all the data in a way that takes into account the human element as well. thank you.

JANIS KARKLINS: Thank you, Volker. Mark SV.

MARK SVANCAREK: Thanks. On E, I was wondering if just changing the word "processing" to "disclosing" makes this work clearer. Is performing a balancing test processing? Wouldn't that be a paradox? I thought the intent of this was perhaps to say you must perform a balancing test before disclosing the data. So I don't know, maybe that's helpful. Maybe I'm missing the point. But it occurs to me that that makes E more effective. Thanks.

JANIS KARKLINS: Okay. Thank you. I think it is indeed. Milton.

MILTON MUELLER: Yeah. So I thought we were discussing E, and is somebody objecting to that being there? So the argument here is very confused. On the one hand, people who are complaining about E seem to be saying they don't want to perform balancing tests. On the other hand, they're saying that machines, these experts in

artificial intelligence are telling us that machines can perform balancing tests perfectly well.

We can set aside the AI argument if indeed machines can perform balancing tests, which is something I would have an argument about, but it's not really relevant because if indeed machines can perform balancing tests, and they are required by law, then E stands. We don't need to change it. we leave it there. Is that correct?

JANIS KARKLINS: Yeah. no one contested that E should go, no. Only the question was whether in case of manual performance or manual disclosure and automated disclosure E would be relevant for automated disclosure in the same way as in the manual disclosure.

MILTON MUELLER: So we're having an argument about automation again, right? Is this the proper place for it?

JANIS KARKLINS: Not really, but it was in the question that ICANN Org put forward.

MILTON MUELLER: All right. Let me just also say that I agree with Mark SV that the word should be "disclosing" rather than "processing." Thank you.

JANIS KARKLINS: That's noted. Thank you, Milton. Eleeza.

ELEEZA AGOPIAN: Thank you, Janis. I just wanted to add a little bit more to my description from earlier. Sorry, I'm still early on my first coffee this morning. I think part of the confusion here was that the recommendation is also referencing automated responses, but there's also recommendations—I think it's recommendation 7 that relates to automated disclosure, should that be possible in the future. So I think we wanted to be clear on whether this comports with what's in recommendation 7.

I think the other area that was a bit confusing to us is that the requirements under A through I apply to both contracted parties and SSAD. And we weren't sure—it didn't quite make sense to us that all of these would apply to all parties even in the case of automated responses, for example, E, which requires a balancing test—

JANIS KARKLINS: But E is where required as applicable law. If it's not required, then the balancing test should not be performed. That's why in others, you have must, and then in E, you have where required. This is a well-crafted point.

ELEEZA AGOPIAN: Sure. I think it just raised some questions for us and that's why we flagged it. So I just wanted to add a little bit more description. Thank you.

JANIS KARKLINS: Okay. And in relation to abuse, I wouldn't like apparent misuse. I wouldn't like to sort of open conversation about that one again. We had in Los Angeles extensive conversation what that constitutes. We created a small group, small group worked and then reported to the plenary. And I think for that clarification, simply, we need to revisit the recording of our last face-to-face meeting in Los Angeles and document—or this is already transcribed, so take it from there, what that meant, this apparent misuse. Stephanie, last word.

STEPHANIE PERRIN: Thank you. I just wanted to put in the usual reminder that while we focus on the GDPR, we must not forget that from a human rights perspective, a charter applies and only the registrars will have the information that would allow you to do that balancing test measuring the impact on human rights, particularly in the case of a government request to the individual.

So to me, we've got to put a stake through the heart of this concept that the SSAD can do a balancing test. It cannot, unless you're going to allow the SSAD to reach into the registrars' databases and get all their financial information in there and their hosting information. Thank you.

JANIS KARKLINS: Thank you, Stephanie. I think we have specific point on this in one of the recommendations. Maybe even this one. But let us move to point three. Caitlin.

CAITLIN TUBERGEN: Thank you, Janis. Point three corresponds to item A which is "must only disclose the data requested by the requestor." And in point three, we've included some of the edits that the EPDP team members that responded to the public comments seemed to agree with, and we put the options here.

There however was a question—and some clarification is needed here because there seems to be an implication in option one where the contracted party could potentially add data to the response that the requestor didn't request, and we were confused by what that actually means in practice.

JANIS KARKLINS: Okay. Thank you. Again, I think we spend hours discussing this. Do we really want to reopen? Kind of obvious, if you request A, if that is permissible, you need to get A, not A and maybe B and then who knows what else. Brian, are you in agreement with me?

BRIAN KING: Thanks, Janis. Yes, I'm in agreement and we prefer the language as it was previously without these edits. Thanks.

JANIS KARKLINS: Okay. Any disagreement to keep the [Chris] formulation as is, return that data that was requested if that is feasible or legal? No objections? Decided. Thank you. Number four, Caitlin.

CAITLIN TUBERGEN: Thank you, Janis. Number four, as you can see, corresponds to B, must return current data. The question that was raised here is about a little bit more specificity about what current data means. And specifically what that means if during the processing of a disclosure request, the data changes or if the domain name is transferred or if it expires, or if, again, the contact information is updated, what data is the contracted party supposed to disclose? Would disclosing the data before it was changed be considered returning historic data, for example?

We also noted that there was a comment that noted that once a disclosure request is received, that the data should be locked similar to a UDRP case. That was a suggestion, but we just needed some clarity about what current data means and some additional guidance.

JANIS KARKLINS: Okay. Thank you. Of course, my immediate question is what is the probability that from the moment the request is logged and information processed, the data would be changed? I think the probability is extremely small. Brian, Mark, and Alan G, in that order.

BRIAN KING: Thanks, Janis. I think here the question is one that we should think about, the concept—I think the concern that could be addressed here is that it's nothing to do with the day that B is worded but what the commenter has potentially pointed out is that if we have a multi-day SLA on this, the concern—which I think is

probably a rare case, but the concern is that the data could be requested and then the data could change after the request was received and before the disclosure of the data happens. So the request was responded to with data that was not the authoritative data at the time the request was made. So it's just a difficulty, I think, with the possibility to have a couple days to process these requests.

So in that case, I think we could probably agree that the data that was authoritative when the request was sent or when the request was received by the contracted party should not be considered historic data and should be able to be disclosed even if the data subsequently changes before the disclosure is made. I hope that makes sense. Thanks.

JANIS KARKLINS: Thank you, Brian. Marc.

MARC ANDERSON: Thanks, Janis. A couple things in this one. First of all, just to touch on the idea of locking the domain is just a nonstarter. That would essentially let any requestor give the ability to hold a domain hostage, any requestor could submit requests and lock the domain, and that's just a nonstarter.

To the question of the data changing, there's probably two different scenarios. There's what happens if the data changes between the time the request has been submitted and the time the contracted party, the person making the decision is able to actually look at the data and make a determination.

So there, it's just—I think the only logical approach here is for the person making the decision to make that decision against the now current data. To have to track a time stamp of when the request was made and then compare the current data against what the data was at the particular time it was requested, that adds a lot of unnecessary overhead. I think we're just dealing with the then current data.

And the other scenario would be if there's any kind of lag between when the determination is made and when the data is returned to the requestor. That is a little trickier, but I think the data returned needs to be the data that the determination to disclose was made against. So I think that could be a little trickier and maybe is worth a clarifying footnote.

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

ALAN GREENBERG: Thank you. I think Marc has just identified the case that's really tricky. If the data changes between the time the request is made and the time someone looks at the request, I think that's life. All we can do is look at the data as it is current at the moment. The real problem is if the data is retrieved and looked at, and a decision is made to release, and the data is changing in that period of time. The mechanism is going to be that whoever looks at it does not type in fresh all of the data to release. They're likely to hit a button to tell the RDAP server to release the data. And it is conceivable that the data has changed since it was retrieved to

look at it. And I'm not sure how we're going to be able to handle that. Maybe RDAP will refuse if the data has changed in the last—RDAP system doesn't know how long you spent looking at the data. You may have spent three days looking at the data. So I really don't know how we handle that situation of the data changing while the inspection is being done, because the release of the data is going to be by the system with the then current data. That's all it has.

So unless there's some mechanism built in to know when the data was retrieved for inspection and the RDAP system considers that, and perhaps bounces the request back to the decision maker, that timing one is a real complex one. Thank you.

JANIS KARKLINS: Thank you. Again, I understand this situation, but I'm coming to my question, what is the probability? How high is the probability?

ALAN GREENBERG: Janis, since these are requests being made about a domain that is in a questionable state—someone is making the request because something funny is going on perhaps—the chances are not all that small that someone else may be reacting to it.

JANIS KARKLINS: Okay. I'm buying that argument. Mark SV, please.

MARK SVANCAREK: Thanks. I think we should focus on the first question that the public commenter made, which is if the policy is must not disclose anything, must not disclose historic data, then the definition of historic data is very important. And they have identified a case where the definition of historic data may be ambiguous, which would make it difficult to comply with the must.

So we need to define what does historic data mean in this particular case. Some people have suggested that you disclose whatever is true in that snapshot of time. We need to define when is the snapshot. Is it the moment the gateway sends you the request? Is it the moment that it lands in your inbox? Is it the moment when you finally get around to processing the thing? We just need to define when that snapshot occurs, when the sampling occurs. That's the current data that gets released, and if it's changed in the meantime, then the requestor has to make another request, which is of course terrible and slow, but I think that's the obvious way around this.

The critical thing though is to make sure that we have an agreed upon definition of when does the data cease being the current data and become the historic data for the purposes of this policy? That's the thing to focus on. the whole suggestion about locking, [inaudible] I don't know who did that, but I think we all agree that that's a nonstarter an would never work anyway.

So let's just focus on the real question. The policy says must only release historic data. What's the definition of that? Thanks.

JANIS KARKLINS: Okay. Can we think of providing some kind of implementation guidance suggesting that the reviewer or contracting party should minimize time of between the examination—or should strive to minimize time between the decision to release data and actual release of data? And that would take care of this particular situation when the data could be changed in-between the time when disclosure decision is made and the time when actual data has been sent to requestor. And again, that would be simply guidance to cover that type of situation. Brian.

BRIAN KING: Thanks, Janis. I put some language in the chat that I think might be helpful. I think Mark SV boiled down the risk here, is that we need to define historic data and exempt the data that was authoritative at the time the request was submitted. Just doesn't make sense to have a prohibition on disclosing that data if it has changed.

I'm not suggesting to require it but I am suggesting that we don't prohibit the disclosure of the data that was valid when the request was submitted. So the language is in the chat there. We can wordsmith from that.

JANIS KARKLINS: But you heard what Mark said from practical point of view. So you submitted request, the request has been treated 24 hours after submission. In those 24 hours, some data was changed by data subject. Now, examiner retrieved the data which has been changed, makes a determination, is not looking when the

timestamps are and then logging information. Otherwise, that adds to workload, especially for the manual processing. So I don't think that your suggestion covers that situation. For me at least, Mark's argument sounded very convincing.

BRIAN KING: Janis, if I could respond, I think in that case we wouldn't have an objection to the reviewer providing the data that they have at the time that they do the review. I think what we're trying to address here is a prohibition that if that reviewer knows the data has changed and would like to send the prior data, the data that was authoritative when the request was received, the reviewer should not be prohibited from doing that. And the language here in B risks prohibiting the reviewer from potentially doing the right thing or the appropriate thing and we don't want to prohibit that from happening. So that's the carveout that I'm trying to get to.

JANIS KARKLINS: Okay. I have staff notice that they have enough material to think about and to fine tune the current text of recommendation for the final reading. But I still have Stephanie's hand up and Georgios'. Stephanie, please.

STEPHANIE PERRIN: Thank you very much. And I don't wish to be overly pedantic here, but be careful how you define historical data. The data that a registrar is obliged to keep depends on local law and that local law is not just data protection law, which varies somewhat widely in terms of how long you have to retain the data, but there are also

certain regulatory requirements and they may have the data in their collection in another form. And I have typed something into the chat a while ago that we never talk about the material that is outside ICANN's remit, but from the perspective of the registrar as a controller of data, responding to a request, they may have data retained for a much longer period. This is why you almost have to separate out the request for active ICANN-related registrant data and historical data. That's part number one.

Point number two, we perhaps could define how long you have to keep a record of a change when we do the IRT. The change in order to respond to accuracy requirements or changes in staff or whatever can be fairly innocuous. We should probably make sure that retention schedules specify how long it has to be retained, because that will give us some uniformity in this manner and it seems to me that it's a requirement.

But that comes in the retention schedules. We haven't talked a lot about those. So, sorry to be nerdy. Thank you.

JANIS KARKLINS: Thank you, Stephanie. Georgios, please.

GEORGIOS TSELENTIS: Thank you. If I understood well something—and please correct me if I'm wrong—we are talking about here a situation where we take a decision based on those called now historic data. So if the decision is a decision of disclosure, I cannot see how we do not give back this specific data that we used for making our decision

and we take int consideration the data that are now in the registrars' database and have changed.

For me, it has to be that the data that we're using for the disclosure are the ones that went under the balancing test, for example, if I take the most difficult case, otherwise we are committing a much more serious problem here, a much more serious fault, because we are taking the disclosure decision based on data that have changed.

So I think the notion here of historic data has to be thought through the perspective that we are talking about the data that were examined and formed the basis for our disclosure decision. Thanks.

JANIS KARKLINS: But this is exactly what we're talking about, Georgios.

GEORGIOS TSELENTIS: Yeah, but I'm saying that that's what we should do.

JANIS KARKLINS: Okay. Thank you. So as I said, staff indicated that they have enough information to fine tune and to make final edits in this part of recommendation, and I think we have covered already five, Caitlin. Don't you?

CAITLIN TUBERGEN: Yes, Janis, we did.

JANIS KARKLINS: We will repeat this conversation that we had. Let's move to six.

CAITLIN TUBERGEN: Thank you, Janis. I agree. So with respect to question six, this again corresponds to item F which is about the data subject [unreasonable] request, getting confirmation of processing of personal data. So on question six through eight, the first two questions were proposed edits put forward. Some commenters raised concerns that the proposed additions could result in contracted parties violating their local laws, but others in the EPDP team requested further discussion, so that's why you see the proposed edits in six and seven. So the team members who haven't read those should probably read through those for discussion.

And then lastly, question eight on this is the clarification on if this requirement is to notify parties whose data is disclosed, or alternatively if this is a notification provided only upon request.

JANIS KARKLINS: Okay. Thank you. So let's take one by one. Number six. So there are proposed edits to the text of recommendation. Recommendation is the one you see in italic and what is in bold is proposed to add. That's my understanding. Brian, please.

BRIAN KING: Thanks, Janis. I'm unclear on the concern presented here and I'd like to understand that better. If anyone's familiar with the concern noted that adding this language might prevent a contracted party from following applicable law, what would that look like and how could we address it? Thanks.

JANIS KARKLINS: Thank you. Somebody from contracted parties can clarify? Or Caitlin? Where this concern came from, who raised it? Alan Woods.

ALAN WOODS: Caitlin, go ahead first. Sorry.

JANIS KARKLINS: Okay. Caitlin, you were ready to answer.

CAITLIN TUBERGEN: I was just going to clarify that I believe this was a concern registered by the Registrar Stakeholder Group, so I would defer to them for this.

JANIS KARKLINS: Okay.

ALAN WOODS: In that instance I'd also defer it to them.

JANIS KARKLINS: Alan. You're deferring to registrars?

ALAN WOODS: [inaudible] registrars, they might be able to give more insight than I.

JANIS KARKLINS: Okay. Marc, your hand is up.

MARC ANDERSON: Thanks, Janis. In just looking at this, I think what we settled at initially in our recommendations was that the contracted parties have some obligation under law to provide information to registrants upon request, how their data has been used, what disclosure requests have been made to their data and how it's been disclosed.

We did not agree on any recommendations that put an obligation on contracted parties to proactively inform registrants. In fact, we agreed that that was not necessary in our recommendations. But by the same token, I'm opposed to a recommendation that prohibits it. So at least on number six, I would be opposed to that language. I think it's not necessary, I think we should leave the language as is.

The one in seven, the changes without disclosing the identity of the requestor, I think this is something we've talked about and covered in other sections. I'm not able to follow it. I think we

specifically considered this scenario when we were talking about maybe specifically to law enforcement. So I think I'm also opposed to this suggested change. I think probably our existing language is already sufficient and this maybe confuses things.

And then I think my comments have already addressed eight here. Is there a need to require to notify parties? I think we agreed there's not. so I think this has already been discussed and we agreed that there's not requirement to notify parties and that this is just—all we've discussed in our recommendations is that it's reactive when the data subject has requested it. I think we can stick with our previous agreement and leave it at that.

JANIS KARKLINS: Okay. Thank you. That would be my preference as well. So, can we follow Mark's suggestion that we simply leave the recommendation as drafted in initial report? I see no hands up. Decided.

Let' go to nine. Caitlin.

CAITLIN TUBERGEN: Thank you, Janis. In terms of item G, one commenter noted that this is redundant of what the law actually states, and is this requirement necessary or can it be deleted? So want to check in on that.

JANIS KARKLINS: Okay. Thank you. Any reactions? Alan Woods.

ALAN WOODS: Thank you. I agree with the commenter at this point, it is redundant to have to say, but at the same time, if we're making recommendations, it should be pretty good for us to say, "And by the way, obviously, the SSAD itself will need a mechanism under which the data subject may exercise its [inaudible] rights." I don't think there's any harm in it, so I would just leave it as drafted.

JANIS KARKLINS: Thank you. Are we in agreement with that one?

VOLKER GREIMANN: Yes.

JANIS KARKLINS: Okay. Good. Everyone is in agreement, so let's move then to ten.

CAITLIN TUBERGEN: Thanks, Janis. For question ten, which refers to H, some of the commenters were suggesting that all SSAD stakeholders should be involved in drafting and agreeing on a privacy policy, but others pointed out that contract language should be determined only by the parties in the contract.

So we are putting forward a possible compromise here. ICANN and the contracted parties will solicit and factor in input from all SSAD stakeholders when drafting and agreeing upon a privacy policy to see if that language might be agreeable. And then also,

we just needed some clarification based on the public comments about who the privacy policy is intended to cover, registrars, requestors or others.

JANIS KARKLINS: Okay, so first question is, are we in agreement with the proposed amendment of the recommendation? Any opposing? Alan?

ALAN WOODS: Apparently I found my voice. I do have an objection to this because at the end of the day, the SSAD needs to be responsible for its own. It's going to be an independent body, it's not as if the SSAD is the community. SSAD is going to be its own entity, one assumes, as part of ICANN. And I genuinely think it's in their interest and it would be in ICANN's interest and in everybody's interest that they draft their own privacy policy with the help of outside legal counsel and not be told how to do it by people who, let's be perfectly honest, might be getting it very wrong.

In fairness, it also took us two years to get to this point. Can you imagine how long it would take us to come up with an actual agreed upon privacy policy for the SSAD? So I think really, it should be based on the law and the applicable law and the place in which it's going to be incorporated, and I really think that should be left up to the SSAD as an entity.

JANIS KARKLINS: Okay. Thank you. Thomas.

THOMAS RICKERT: I guess it might be worthwhile noting for the commenter that the contents of a privacy policy are not policy. We are dealing with legal requirements that are derived from statutory law and therefore I think this is neither a community exercise nor are the contents up for discussion. We could clarify through one to two that the privacy policy needs to cover all minimum requirements established under the GDPR, but I guess that other than that, we're seeing that this group had a challenge to combine policy with compliance, and this particular [one] is no policy but pure compliance.

JANIS KARKLINS: Okay, Thomas, thanks. Margie.

MARGIE MILAM: I think I have a different perspective regarding this. I do think that in the end, ICANN and the contracted parties will—well, actually, there's a difference here. With respect to the SSAD itself, I do believe that there should be public comment on it. it doesn't mean, obviously, that everything that comes in a public comment gets represented in the privacy policy, but I think it's a checks and balances, if you will ,and because the SSAD is a global resource—or it will be when it's set up—we might very well see input from different parts of the globe as to what it should say. So I do think it's useful and it's part of the overall ICANN process to ask for public comment. I think that's all really what this says.

JANIS KARKLINS: Thank you, Margie. Mark SV.

MARK SVANCAREK: Thank you. Alan is raising or maybe hinting at a point that he had also made in LA, namely that the privacy policy of the SSAD may be different from the privacy policy of the contracted parties in that the contracted parties' privacy policy points to the policy of the SSAD. It seems that the privacy policy of contracted parties would be negotiated solely between them and ICANN whereas the privacy policy of the SSAD—now I'm thinking I agree with Margie, it's something that would require public comment and feedback solicited and factored in, but it would be a separate thing. And I think perhaps that those things are being conflated here, so Alan's distinction is important and might need to be clarified. Thank you.

JANIS KARKLINS: Okay, so I heard support to proposed amendment and opposition to proposed amendment. So [got nothing in this] situation and we need to think what would be way out of opposing positions. Marc Anderson, please.

MARC ANDERSON: So I think Mark raises a good question. Are we talking about the privacy policy of the SSAD or are we talking about the privacy policy that registrars have with their data subject customers? And I think we're talking about the second, in which case, I think Thomas—I couldn't add anything to what Thomas said. But based on what some commenters have said, I think we're not in

agreement on which privacy policy we're talking about. So maybe we should clarify that fist.

JANIS KARKLINS: At least for me, it's clear it is a privacy policy for SSAD.

MARC ANDERSON: So the language may be a little misleading. I don't think that's actually what it says.

JANIS KARKLINS: At least this was intended to say, because in SSAD, we'll handle the private data. So as a result, system itself should have a privacy policy that everyone subscribing to use SSAD also should subscribe to.

MARC ANDERSON: In that case, the data subjects that we're talking about are the requestors, the users of the SSAD, which is a very different question than what goes on next, to be presented to data subjects by the registrars, which really implies that it's the registrants that we're talking about.

So I think what I'm saying is we need to clarify, the registrants would not be presenting a privacy policy to SSAD users. You see what I'm saying? So it's not clear—and I think what we're saying is this is not clear if we're talking about the SSAD privacy policy that would apply to users of the SSAD or if we're talking about the privacy policy that would go to registrant data subjects my

registrars. I think we're not going to be able to agree until we understand which privacy policy we're talking about and who it's applicable to.

JANIS KARKLINS: Okay. Let me then maybe—I will collect further inputs and I will solicit staff to reflect and make it abundantly clear in the final version of the recommendation what we are talking about here. If need be, please, they will consult relevant stakeholder groups who put or who raise questions, and then they will provide very clear statement for the final reading. But in the meantime, Laureen and then Stephanie.

LAUREEN KAPIN: Thanks, Janis. In reading this, it seems to me that the privacy policy would be applying to the users. That's something that they would be getting notice of before they decide to provide any information. And I agree it's confusing because it talks about data subject and we're typically thinking of the registrants as the data subject, but I think Marc's point is well taken that this is a heads up to the users of the SSAD as to how their information will be treated. That said—and I'm wrong, I'm wrong—I think the two approaches that you said were in conflict, perhaps it could be resolved by a matter of sequencing, that as Alan and Thomas had suggested, this could be something that ICANN Org handles in consultation with its legal advisors as to what type of privacy policy would comply with the law and then thereafter, public input via public comment process could be sought, especially if there was a desire to go beyond the law on certain issues that certain

stakeholder groups deemed to be important. So that's just my suggestion to resolve this, what I don't see as a conflict but more a matter of sequencing.

JANIS KARKLINS: Okay. Thank you. Stephanie.

STEPHANIE PERRIN: At the risk of being a broken record again on this, I have complained many times that we're going at this backward, and this is a fundamental question that would have been good to have addressed at the very beginning by a privacy impact assessment and legal analysis that established where there was ambit —if you're drafting a privacy policy, obviously, you sketch out the parameters of what's required in the law, some of which are not open to question.

Others have a great deal of ambit, and that's where you put ancillary policies in place. I would think it very inadvisable to have many privacy policies. This SSAD is a disclosure instrument to describe to individuals how you are disclosing their data to third parties. It is an area where there is properly some ambit and some best practice, but there's also a lot of law that constrains disclosure.

So in my view, having a separate SSAD policy for disclosure only is once again a replication of the old WHOIS. In a similar manner, you have to drag the escrow agreements and requirements that ICANN quite correctly sets policy for into the same registrant data policy, harking back to the old EWG effort that was labeled the

RDS policy. If we're talking about registrant data, we have to look at it all, and we also have to revise the thick WHOIS policy because that in my view is no longer justifiable unless you come up with a whopping competitive argument that ICANN would have a responsibility for, and I certainly didn't see it in the recent review of competition.

So all of these things have to fit in one policy. You're not going to have 15 policies and force the poor individual to seek his way through different policies to see how his data is seeping out of ICANN. Thank you.

JANIS KARKLINS: Okay. Thank you, Stephanie. Thomas please.

THOMAS RICKERT: Thank you very much, Janis. There's been some discussion around privacy policies of registrars versus the ones for the SSAD. Certainly the registrar operates processing activities that don't have anything to do directly with what ICANN is doing or what the SSAD is doing. However, the registrar is the interface to the data subject, and therefore, the registrar needs to make sure that all the information pertaining to article 13 of the GDPR is presented to the data subject at the time of collection. So that's going to be a vital part.

So even if presented by the registrar, it will be the registrar that has to present the privacy policy describing what's happening in the SSAD to the data subject. Otherwise, we would be in trouble with all this.

Having said that, a privacy policy describes the policy on processing the purposes, the legal bases and all of that which we are preparing in this exercise and therefore it's more like a [clerical] or legal craftsmanship type activity to put our recommendations into a privacy policy that needs to be used for the data subjects. And therefore, I would caution against making this a community exercise where community members might think that they can rehash arguments over what processing activities will take place and relitigate some of the arguments that we had. So I think that this product as we're currently doing is one that need sot get public comment, but the privacy policy is just a mechanical side product of that. And I think therefore, if there are concerns by some in this group that the privacy policy might not accurately reflect the contents of our policy and recommendations, then it would be a matter for implementation oversight, but not for soliciting additional community feedback.

JANIS KARKLINS: Thank you, Thomas. I think indeed, there need to be simply clarification in this subpoint H. Maybe staff can think what would be the best way to reflect that. So first of all, with SSAD, when SSAD will come to life, there is a requirement and this is said in the first sentence of this recommendation, that data subjects should be informed that third parties may get access to their data in certain circumstances. So that's the one element.

The other element is that SSAD itself should have this privacy policy which is based on article 13 and 14 of GDPR and that should be crafted, as Thomas said, by lawyers in the best possible way, [and applied.] I think that these are two elements that I

understand we want to cover here and maybe there is a way how to find a way how to separate them in this subpoint H, maybe with two separate bullets under the same bullet point or so. Staff, please, you have enough material to work on. Would that be okay? Good.

So now we can go to 12. Caitlin.

CAITLIN TUBERGEN: Thank you, Janis. Question 12 corresponds to point I, which is the confidentiality of disclosure request, and 12 includes the proposed edits that were put forward for the team's consideration. But we wanted to note that a concern was expressed that it would be very difficult to apply confidentiality to nongovernmental agencies, and we wanted to see if there was a way forward on this.

JANIS KARKLINS: Okay. Thank you. Any thoughts? Marc Anderson, please.

MARC ANDERSON: Not so much as a thought, as a request. I recall maybe my recollection was that I was the result of some work between Chris and James to come up with this language, and since James isn't here, can I put Chris on the spot to ask him to weigh in a little bit on his thoughts of these proposed edits? My inclination is that I like the existing language better, but I would love to hear from Chris on the proposed edits.

JANIS KARKLINS: Okay. Thank you, Marc. Chris.

CHRIS LEWIS-EVANS: Yeah. Thank you, Janis, and thank you, Marc. To be honest, I seem to think that the language in I is different to the ones me and James suggested because there was—oh, no, sorry, it is there.

JANIS KARKLINS: No, Chris, the original language is in italic.

CHRIS LEWIS-EVANS: Yes. Sorry.

JANIS KARKLINS: And that is what you suggested. The only unresolved issue is whether to use “and” or “or” in the last line.

CHRIS LEWIS-EVANS: This makes it massively complicated. It'll be a real problem when it comes to implementation to actually—how do you implement that into policy, this recommendation? It would need a fair amount more work to be able to fit in some of these concerns into language that I think we would be happy to pass as a group, and I would need to have a discussion with probably someone on the registry/registrar side to be able to get it to that point. So I think the language there is not implementable, so maybe something for me and James to have a look at off this call.

JANIS KARKLINS: Okay. So in other words, you're not in favor of changing initial language from the initial report on I.

CHRIS LEWIS-EVANS: Correct. I think that covers most of the concerns.

JANIS KARKLINS: Thank you. We still need to think about and or or.

CHRIS LEWIS-EVANS: [inaudible] actually on the last calls on this, but without James here, it would be harsh for me to recommend.

JANIS KARKLINS: Okay. Let me take Milton and then Laureen.

MILTON MUELLER: Yes. I agree that we do not want to make these changes, in particular the two bullet points I think open a huge can of worms and basically are designed to massively limit almost o the vanishing point the right of data subjects to actually get disclosure about the disclosure of their data. So I would oppose that. And I agree also that it should be “and” rather than “or” on the bottom.

JANIS KARKLINS: Okay. Thank you, Milton. Laureen.

LAUREEN KAPIN: I don't have a problem with the language as it's written, but in terms of implementation notes, I would agree with the first bullet point coming from the perspective of the civil law enforcement agency who does require confidentiality. I think it is a useful point to highlight that criminal investigations are not the only types of investigations that require confidentiality. That said, I'm not going to press for a language change, but I do think in terms of implementation, to the extent that there is ambiguity here, that that point should be clarified.

JANIS KARKLINS: Okay. Thank you. That's helpful. Margie.

MARGIE MILAM: I prefer the change here, entity versus authority, because there are times when private parties are cooperating with law enforcement on investigations or civil investigations, and so I would want to make sure that that is still possible. It doesn't say that you have to have it dealt with confidentially, it just says "may." So I think the language that's proposed here is preferable.

JANIS KARKLINS: Sorry, which specific language you're talking about?

MARGIE MILAM: Accepting the change of requesting entity instead of requesting authority.

JANIS KARKLINS: Can I have it highlighted on the screen? Ah. Okay, can we think of—as Laureen suggested, maybe not to change the initial language of the recommendation but add some additional language and implementation guidance which would reflect also civil investigations that may require some confidentiality. Alan.

MARC ANDERSON: Thank you, Janis. To be honest, I'm trying to digest this at the moment. I think just when we are doing this, we need to be very clear that we can only override the data subject request, which is the legal right of the data subject, where there is specifically something written in law that applies to us as the controller that would prevent us from doing that.

It is not an absolute right, absolutely, but at the same time, I think it needs to be clear that there needs to be a power somewhere that says, yes, you cannot disclose this to the data subject. And I don't think that's covered enough in this. But I agree that it's not just limited to criminal, there are other areas in which it could be an obligation of confidentiality. I just think we need to be certain that it can't be just claimed, it must be demonstrated that they have that right to deal with confidentiality. I know that doesn't help but I just wanted to be clear on that.

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

BRIAN KING: Thanks, Janis. I agree with Margie and Alan Woods. This would certainly not be an every case scenario, but there r a number of applications of this where the law might support preventing the disclosure to the data subject. Probably shouldn't have said disclosure. Shouldn't [inaudible] right of access that are perfectly grounded n law outside of criminal law. So I would definitely support the inclusion of the civil language here. Thanks.

JANIS KARKLINS: Okay. Thank you. I got indication from staff that they have enough information to try to edit the recommendation as a result of our conversation.

So on 13, Caitlin, what's the problem here?

CAITLIN TUBERGEN: This is another commenter that expressed concerns that in certain cases, local law requires disclosure to a data subject even if the requestor has requested to be treated confidentially. So we added here, should a note be added that this is subject to applicable law to address the concern of the commenter?

JANIS KARKLINS: But isn't that covered already with the last part of this last sentence? An initial confidential request maybe disclosed to data subjects in cooperation with the requesting entity and in accordance to the data subject's rights under applicable law. That's fully covered already. Do we really need to have a conversation about it? Chris.

CHRIS LEWIS-EVANS: Yeah. Thank you, Janis. I think you just made my point for me, and the reason why we want the and in there, because that would cover that off nicely. Thank you.

JANIS KARKLINS: Thank you. So, any objection? And then 14 is and/or. Chris suggestion was to settle on “and” supported by Milton, and I understand from Chris that that was also something they discussed with James. So my suggestion is simply to put it “and” as per Chris’ suggestion. Objections? No. Thanks.

So, do we have something else here? We don’t. So on issues that we couldn’t come to final conclusion, staff will do the writeup, edits, and we will look at them during the last reading of the text with a “can or cannot live with” method. So with this, thank you. I think now we can move to next recommendation. We still have some 15 minutes in the call, and that is recommendation 6. Caitlin, please.

CAITLIN TUBERGEN: Thank you, Janis. For recommendation 6, the first question that we had, one of the commenters noted that there should be additional guidance provided in terms of what sort of third-party providers the contracted party may outsource the authorization responsibility to. So here we’re just looking, is this something that the team agrees needs further clarification? Or if similar to the identity providers noted in recommendation 1 on accreditation, if this is something that should be sorted out in implementation.

JANIS KARKLINS: Okay. Thank you. Any comments? Brian.

BRIAN KING: Hey Janis. Thanks. I'll just note that the chat is violently agreeing that this goes to implementation. Thanks.

JANIS KARKLINS: Okay. No further recommendation. Marc Anderson, please.

MARC ANDERSON: I would maybe go a step further. I think this is something that should be left up to the contracted party. I'm not sure there should be any restrictions either in recommendations or in implementation. I think it's ultimately a contracted party decision on what and how they would outsource this.

JANIS KARKLINS: Specifically because of the second part of the recommendation which suggests that "but the contracted party will remain ultimately responsible for ensuring that the applicable requirements are met?"

MARC ANDERSON: Yes, agreed.

JANIS KARKLINS: So, can we settle not to do anything further than this and let contracted parties sort it out? If they decide to outsource the risk of 4% of turnover. Okay. Decided. Number two. Caitlin.

CAITLIN TUBERGEN: Thank you, Janis. So beginning in section two, the question here is that one of the commenters noted that in this recommendation, contracted parties should be changed to controller. I'll note that one of the EPDP team groups was not okay with that change but noted that maybe contracted party controller would be acceptable here. And we wanted to see if this was something that the team agreed with and if the recommendation needed to be changed throughout, but we wanted to note that this recommendation is related to contracted party authorization.

JANIS KARKLINS: Okay. Thank you. So let's take one by one, question two. Brian.

BRIAN KING: Thanks Janis and thanks, Caitlin, for clarifying that this is in the contracted party section because my response might have differed. But if we're talking about that, then I would not change to controller without any agenda whatsoever except that I think we can't agree on controller, nor is that decided or clear right now. So if we mean contracted party, let's say contracted party here. Thanks.

JANIS KARKLINS: So contracted party is in the title. And just to refresh memory—and [I'm talking, I'm the controller of the staff,] this comes from this very elaborate sort of sequence of actions that need to be taken to make this disclosure decision that I think Alan put forward initially and then we based this recommendation on that practical way how contracted parties make disclosure decision.

So number two is decided. Number three? [Should provide with change demonstrated in the first bullet and the four] so it would read the requestor demonstrated legitimate interest or other lawful basis in processing data. Any problem? For me it sounds like editorial change, provided, demonstrated. Any objection to change from provided to demonstrated? No objection. Will be changed.

Number four, determination should consider elements how can inconsistent interpretation be avoided of what requestor must provide. So, any comments? I think we spent hours and hours discussing this particular recommendation. Let me see. Marc, your hand is up.

MARC ANDERSON: Thanks Janis. Looking at the questions, I'm not sure what we can do to address these. I think we've done the best we can with these and I'm not sure I can think of edits to the—so if anybody has any other thoughts or suggestions here, we could consider them, but I think absent suggested edits, I don't know how we can tackle these questions.

JANIS KARKLINS: Okay. Thank you. So then, may I take that we are not willing to change anything in this first part of recommendation that we see in italic on the screen? Okay, so let us then go to six, seven and eight. Caitlin, what is here?

CAITLIN TUBERGEN: Thanks Janis. These questions once again correspond to the phrase, if the answer to any of the above questions is no, the contracted party may deny the request or require further information. So these questions deal with requiring further information and denying the requests. The first is that this question six deals with a comment about if the contracted party does deny the request, should there be an ability for the requestor to appeal? And the question is what should the appeal look like and who would be the arbiter. I'll note that in the contracted party response, they say that the arbiter would be the DPA.

Question seven is about if there should be an intermediate step before the official denial of the request. I'm sure the requestors have the opportunity to provide more information. And then lastly, question eight was a question from ICANN Org and the EPDP team members that responded to this noted that further implementation guidance should be provided in relation to contracted parties going back to the central gateway to request more information and how that interaction should happen. But the groups that agreed that we need some high-level implementation guidance didn't provide any examples in the discussion table, so we need some examples here.

JANIS KARKLINS: Okay. Thank you. Margie.

MARGIE MILAM: I do feel a little uncomfortable that we're moving so quickly through these topics. I think the concerns that were raised in the questions above and here really get at the question of whether or not there's an ability to challenge the decision if the decision is wrong. For example when we did the change of "provided" to "demonstrated," I think that change may have come from us and we want to make sure that there's some sort of reasonableness associated with it.

So I think, yes, the change to demonstrated causes me a bit of concern as I think about it and would like to suggest that it says something like reasonable provided or some sort of element like that so that there is an ability to have a decision addressed if it's just wrongfully denied.

JANIS KARKLINS: Okay. Thank you, Margie. Marc Anderson.

MARC ANDERSON: Thanks, Janis. I'm kind of noting the time. I don't know, we have less than five minutes, I don't know if you maybe want to cut me off and we can continue the discussion later.

JANIS KARKLINS: No, go ahead. Just tell what you want to say and then seems that we will need to stop the conversation here. But please go ahead.

MARC ANDERSON: Okay. Fair enough. So my comment was on question number eight. I think these are good questions that we maybe want to spend a little bit of time with, sort of the—we're not very clear on how a contracted party might go back to the requestor when the contracted party doesn't have a direct line of communication with the requestor. So I think this is a good question we maybe need to spend a little bit more time on. And there's some other considerations with both seven and eight. So how SLAs would be considered if there's back-and-forth between the requestor and the disclosing entity. I think these are good questions but maybe require a little bit more thought. Probably thought that would apply to implementation guidance, but I think these are good questions we need to spend more time on.

JANIS KARKLINS: Okay. Thank you. So this is what we will be doing first thing during the next call. Brian, something burning?

BRIAN KING: No. Can wait until the next call. Thanks, Janis.

JANIS KARKLINS: So we will then restart from six next time. And of course, last time we discussed briefly about the appeal mechanism, and one of the options was to see whether appeal mechanism could be attached or be part of the evolutionary mechanism that we are working in the small group, and hopefully meeting for the last time tomorrow

prior to putting the proposal for the consideration of the team afterwards. But seems that this evolutionary mechanism may not be the right avenue for any appeal, so therefore, I would like maybe to invite who can—maybe from BC, IPC, one, and then from contracted parties house one volunteer to think until the next call what this appeal mechanism could look like, but also being very pragmatic that this is something we could consider.

And before I close the call, I have a question to the GAC representative about the accreditation of public authorities. Can we, or when can we expect your input? Sorry to put you on the spot now but it's for planning purposes very important. Anyone from the GAC hiding? Please, let me know as soon as you can.

So with that, that brings us to the end of the call. Thank you very much for constructive participation. As you see, the agenda for the next meeting is already shaping up. We will start with recommendation six—continue recommendation six and we'll take up authorization, automation recommendation for considering by EPDP. And so you'll get the homework immediately after the call. And with this and in absence of requests for the floor, I would like to thank all of you for active participation in the meeting. This meeting is adjourned. Have a good rest of the day.

VOLKER GREIMANN: Bye.

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

[END OF TRANSCRIPTION]