ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2
Wednesday, 04 December 2019 at 14:00 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.
Attendance and recordings of the call are posted on agenda wiki page:
https://community.icann.org/x/DoEzBw
The recordings and transcriptions are posted on the GNSO Master Calendar Page: http://gnso.icann.org/en/group-activities/calendar

TERRI AGNEW: Good morning, good afternoon, and good evening and welcome to the GNSO EPDP Phase 2 team meeting taking place on the 4th of December 2019 at 14:00 UTC. In the interest of time, there will 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 Ben Butler of SSAC and Brian King of IPC. Also, Chris Disspain will be joining us a little late. They have formally assigned Tara Whalen and Jennifer Gore as their alternate for this call and any remaining days of absence. Alternates not replacing a member are required to rename their line by adding three Zs to the beginning of their name, and at the end in parenthesis, their affiliation-dash-alternate which means you 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 chat or use any other Zoom room functionality such as raising hands, agreeing or disagreeing.

As a reminder, the alternate assignment form must be formalized by the way of the Google assignment form. 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 email the GNSO secretariat. All documentation and information can be found on the EPDP Wiki space. Please remember to state your name before speaking. Recordings will be circulated on the mailing list and posted on the public Wiki space shortly after the end of the call. With this, I'll turn it back over to our chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you. Thank you, Terri. Good morning, good afternoon, and good evening. Welcome to the 32nd team meeting. So, you have in front of you on the screen the agenda of combined 32nd and 33rd meeting. I would like to see if there is agreement to follow proposed agenda during today's and tomorrow's meeting. I see no objection, so we will do as decided. So, thank you very much.

The first sub-item on item three is update on the work of the [inaudible] committee, and if I may ask Becky to give us a brief on the progress. Becky?

BECKY BURR: Thank you. Yes. we met yesterday. We have finished working through the first set of questions and are working our way through the tier questions. We will have some questions coming to the full

EPDP for consideration in the next week or two. We've also received Bird & Bird's comments on the draft summaries of the legal opinions. The legal committee is reviewing those internally, and assuming that everybody signs off, they will be circulated to the full EPDP at the end of this week. And I think that's where we are, working away.

JANIS KARKLINS: Okay, thank you. Do you have any idea when you would report that the work of the legal committee is completed?

BECKY BURR: Well, we still have some work to do on the second tier questions. So, my hope is that we iterate with the first tier questions, get those completed and out to the EPDP but really we just started on the second tier questions on our last call. So, we've had two calls on it. We are trying to, by topic, take all of the various questions from various places. So, questions on legal versus natural person have come in from registry and registrars, from GAC, from IPC, trying to put those all together and streamline them so that we have a consolidated set of questions on each topic as opposed to seven different flavors of the same question.

JANIS KARKLINS: Okay, thank you. Any questions to legal committee at this moment? So, thank you very much, then, Becky. We're hoping to receive the formal legal questions for review as soon as you are ready. Thank you. So, let me now to move to next sub-item and that is building blocks. But before doing that, I see that there is welcoming stream in chatroom to welcome Frank. Frank replaced Alex in the team. So, Frank, if you would like to say a few words, that we familiarize ourselves with your voice, then this would be the right time.

FRANK CONA: Good morning or good afternoon, everyone. I'm based in Washington, DC. I work for the Motion Picture Association. Other than my voice, you should know that I'm fully aware of how irreplaceable Alex is, to whom I'm eternally [inaudible]. I'll try my best not to disappoint. Thank you.

JANIS KARKLINS: Thank you, Frank. Okay. So, status. Status report. You see we have a few things still to do. So, let me now go to the next agenda item. That is issues related to our work, and specifically draft initial report that was circulated to the team as a Thanksgiving gift, and it seems to me that it was not sent back during the Black Friday.

But jokes apart, we have this draft report which also was posted as a Google Doc for comments and input. We have received a few. But before going into substance, I would like to say maybe a few words in explaining, thinking of my own in relation to further work and progress.

So, we have done a lot and we still have a few things to [inaudible] and then of course we do not have common position from the mental things, like a model of centralized hybrid or decentralized.

That said, these things, in a great extent, depend on input that we, at one point, will receive from European Data Protection Board that will inform our discussion. We thought that, while we're waiting, those inputs we could think of presenting initial report with the certain options. And I understand from the staff that initial report outlining certain options or formulating certain questions would not be novelty, that that has been done also in other PDPs and that has not created much difficulty.

So, let me tell you if we can get the timeline on the screen. So, we still have some four meetings to go now in December, including these two today/tomorrow. Then next week and one week after.

Of course, if we opt for the second option, if we could get the next slide, going into January, we would have additional four meetings for online meetings and then we would have three days during the face-to-face meeting.

So, the initial report, in my view, is about 70-75% ready. We may get with the meetings in December maybe to 80% readiness. The rest would be in forms of options or questions. So, if we would consume time until face-to-face meeting, there is no guarantee that we would get to 100% readiness anyway, so we would still may have some open issues and we would not be going to put, again using the same arguments, that it is not 100% ready.

Then, if we look to the overall timeline, can I get the next one? So, this is just a list of … This one is important. You see, if we look to what is named as the current plan, we have a chance of producing the final report by April. And if we follow the scenario, too, where initial report would be submitted by end of January as a result of face-to-face meeting, there is a projection that final report could be completed for the June meeting of ICANN. But there is no guarantee. There is no question if something happens in between we go beyond June meeting. That is the risk.

If we strive to present initial report now in mid-December with a clear understanding that this is not ideal and not fully agreed initial report with [inaudible] questions, so then we have a fairly good chance that the final report would be presented to June meeting.

So, with the second scenario, there is no such guarantee. So, that's simply our best assessment based on previous experiences and taking into account that unexpected things will happen in life.

The only reason why myself and support staff are really suggesting to do this last push and get initial report out, that we can concentrate on unresolved issues and priority two issues. And then get to the face-to-face meeting with a full agenda to finalize report and start looking into comments which then would be submitted during the public comment period. So, this is our thinking, but of course I am not insisting—please do not consider that this is going to only push and only option. If team wants to take time, [inaudible] in your hands. I must tell you today I learned that on 22nd of June I need to be in Geneva which means that if I will go to June meeting, then it will be Saturday and Sunday, flying back Sunday night to be in the morning in Geneva and do my professional duties in Geneva starting the 22nd at 10:00 AM. So, that is another thing that I wanted to inform you that you are aware also my limitations.

Now, floor is open for any comments. I would not like to take the next 15 minutes. So, please, Alan Greenberg is first to speak. Alan?

ALAN GREENBERG: Thank you very much. As much as I appreciate the risks of scenario two and certainly scenario three, I just don't see how we could get out a report that we can stand behind in the next eight days. There's a huge amount of work that is still unresolved. Review by the various groups. It's highly unlikely we'll get comments that we can stand behind and have them incorporated in that timeframe. I just don't see any possible way that we could do this and have a report that I think will be worthy of the quality that it needs to be based on what's at stake in this whole overall process.

So, there's just not enough time between now and eight days from now to publish a report that has both quality and reflects the feelings of the groups. And for better or worse, there's no way I could do an all-day meeting, especially given that for some of us it would likely not be in particularly good hours. Among other things, for some of us, anyway, the PIR ISOC thing has suddenly taken up a huge amount of time which wasn't scheduled by anyone. I just don't see how we could proceed on that timeline. Thank you.

JANIS KARKLINS: Okay, thank you, Alan. So, there is no further requests for the floor but there is traffic in the chatroom which suggests to me that there is an overwhelming support to Alan's statement. So, let us then move on. It seems that scenario has presented in current proposal will not fly. We will then work on assumption of the scenario two.

That said, I of course, personally, I regret but I understand and, as I mentioned, I am in your hands and I hope that report end of January will be the one that we can sign off with all of us as our [consensual] report. James Bladel, please.

JAMES BLADEL: Hi, thanks, Janis. Hopefully, everyone can hear me.

JANIS KARKLINS: Yes.

JAMES BLADEL: Just want to … Can we go back to the slide—Barry, I don't know if you could put the slide up where you have the three scenarios. Wow, that's a nice car.

I think what some of us were saying, discussing in registrar and registry group was that it may be possible to stick with scenario one, the current plan, with a number of provisos and qualifications, and the first one being that we acknowledge the incompleteness and the omissions in the initial report.

The second one is that we commit to a second round of public comments sometime in that timeframe. So, the final report completion date probably moves out. I know Janis has said he has a commitment in June. I'm a little jealous. I kind of wish I knew my commitments that far in advance but I'm sure something will come up.

I think the other part of it would be … One thing that might expedite our public comment period—and this is a controversial proposal—is this idea that, while no one can stop individual companies and organizations and people from commenting during a public comment period, it would be really interesting if the folks on this group could convince their stakeholder groups and constituencies to stand down a little bit during that first comment period.

Agree or disagree, I think one thing is true, that we all very acutely understand the positions and concerns of the different stakeholders that participate in the EPDP. And it might be a good opportunity to use that first comment period to really get input from folks who are not following this process closely and not participating on a daily basis rather than just using it as an opportunity to restate things that we've been discussing for a couple of years now.

So, that was my thought here and I don't know if I'm speaking ahead of my skis here for the registries and registrars, but I thought that there was a path that could get us closer to scenario one—call it scenario 1.5—where we hit the initial date but we push out the final report. I thought that would be something worth discussing. But I also wanted to make that proposal about the initial comment period because I think we could change how it's used and make it much more valuable. Thanks.

UNIDENTIFIED MALE: Janis, you may be on mute.

JANIS KARKLINS: I am on mute. Thank you. Thank you, James. I think we have to … At least this is what I was told, that we have to follow existing procedures and existing procedure suggests that there should be a comment period after publication of initial report but then there should not be public comment period prior or after publication of final report provided that final report does not contain totally different ideas that were expressed in initial report.

So, as a result, if we do not want to proceed in a way as we suggested, then let's take another ten meetings and finalize initial report in a way that we all feel comfortable and then put it out for public comment and then see what will come up. By then, of course, we may know some unknowns of today, like position of European data protection agency that we were told that may come sometime December/January without specific commitment about financials. That is something I do not know. Maybe that is the question to ICANN Org liaisons to find out when potentially we could expect any rough estimate of financials, because if that is an obstacle, then that may influence also release of initial report, should these numbers come late or are not coming for the expected time of release of initial report end of January.

So, honestly, I do not really see a big added value of going for two reports and then two comment periods. Berry, your hand is up. Please, go ahead.

BERRY COBB: Thank you, Janis. I couldn't be remiss without bringing in some of my wet blanket comments. So, for sure, scenario two is possible within the end of the fiscal year but that means we have zero slack in the rest of the time. That means that when we do launch the public comment period at the beginning of February, that it's a strict 40 days. That means that there's still time to review those comments and of course then there would still be considerable amount of time to complete the activities we need into a final report. But note that in that realm, what would be the Kuala Lumpur meeting, there is no time for face-to-face discussions. At best, the report would already have to have been submitted to the GNSO Council. At best, this group would be presenting on those recommendations to help further inform the community.

The last thing I'll say, in terms of public comments, according to the operating procedures, there are no limitations on the amount of public comments. The only requirement is that an initial report must go through the normal public comment process and procedure. Thank you.

JANIS KARKLINS: Thank you, Berry. Maybe in a case of scenario two, we need to think whether sometime end of May or early June we should not think of either additional physical face-to-face meeting or additional virtual face-to-face meeting in order to finalize this final report. Again, I'm just putting this out as a question mark for further consideration when we will get there.

So, Alan Woods.

ALAN WOODS: Thank you. I just want to point out something. I appreciate, and absolutely appreciate, that this is a very complex dance when it comes to timings and things like that. But again, our goal here has to be the quality of the work and not creating outputs just because we have a particular limit on us. And I appreciate that there are outside factors. I appreciate there's expectations, but those expectations will be sorely missed if we put out something that is not fit for consumption. And I think that's the problem.

So, I appreciate what Berry is saying and I appreciate it's going to be difficult, but our core concern should be the quality of what's in our deliberations and not necessarily trying to fit in within false constructs of timings. I know it makes it harder but I think we need to make sure that our focus is in the right way and that is on the quality of the output, not necessarily on meeting people who aren't involved in this day to day on their expectations.

So, I just wanted to say that on the record because I think it's exceptionally important that we get the [inaudible] from this.

JANIS KARKLINS: Thank you, Alan. No, I agree. No question about it. Simply my worry is that, because we may not know outside the responses also at the end of January. It may happen. So, what we will do then? Then we will repeat this conversation and we'll need to decide [whether to] put out report containing options or wait and then we are completely off any targets that have been suggested.

Anyway, I would say let's put a close to this conversation. The direction and the [mode] is clear. We keep working. We do our best. We go with the proposed plan, and now if ICANN asked to put back those dates, simply to visualize—next slide, please.

These are the dates [and now please look] to extend adoption. So, this will be our schedule for our activities leading towards the face-to-face meeting 27, 28, 29 of January in Los Angeles.

So, with this, let's move to response requirements. Response requirements. We got through A, B, C, D. I need now to help … So, we deleted point which required a reporting—unnecessary reporting—and we are now … Didn't we delete D? Caitlin? Didn't we agree to delete and [inaudible] responsible for responding? We'll provide the report to ICANN Org with [inaudible] number of requests and so on. Could you remind us, please?

CAITLIN TUBERGEN: Hi, Janis. And I apologize if we did agree to delete D and we neglected to do that. We can do that in the next iteration of this building block.

JANIS KARKLINS: This is the previous one, the one which requires reporting. I'm not looking in the screen, actually. I'm looking in my computer. Okay, this is what we agreed. These now in the format that we preliminary agreed and then closed it during last meeting.

Now we need to go to E and then the rest of the text. So, E. A separate accelerated timeline will be recommended for response to urgent SSID requests. Those requests for which evidence is supplied to show an immediate need for disclosure. The criteria to determine whether it concerns an urgent request are limited to circumstance that poses and imminent threat to life, serious bodily injury, critical infrastructure, and child exploitation.

So, we started that conversation but we didn't finish. How do you feel about that? Margie?

MARGIE MILAM: I think the list is too restrictive. It should also include things like serious financial harm, like a phishing attack as an example.

JANIS KARKLINS: Thank you. Marc Anderson?

MARC ANDERSON: Yeah. It's just a procedural question, I guess. I put a Google Doc link in chat and I'm just hoping if staff can confirm that I'm looking at the right version of the Google Doc that we discussed in ICANN.

CAITLIN TUBERGEN: Janis, I can answer that question.

JANIS KARKLINS: Yes. Please, go ahead.

CAITLIN TUBERGEN: Yes, Marc, the hyperlinks that are on the Wiki page, which I see Berry is now showing, resolve to the building blocks that everyone should be looking at. And I'll note that support staff went ahead and put the updated text from the initial report where applicable at the beginning of every building block.

And as noted in an email that was previously circulated, the orange highlighted text either represents placeholder text that support staff tried—or endeavored—to resolve some of the issues or text that EPDP members had issues that they had previously flagged or text that we haven't yet gone over.

So, if you look at the top, it says initial report text. That's the text everyone should be looking at and we should specifically be focusing on the orange highlighted text. Thank you.

MARC ANDERSON: Great. Thanks, Caitlin. That's very helpful.

JANIS KARKLINS: So, any further questions, Marc, or specific comments on this subpoint E? Margie suggested to add financial crime—serious financial crime.

MARC ANDERSON: Sorry. I'm just trying to make sure I'm on the right page right now.

JANIS KARKLINS: You can see also on the screen. It's subpoint E. Look, I will take James and then I will come back to you. James?

JAMES BLADEL: Thanks, Janis. I disagree with Margie. I don't believe that winding this is the right approach. I think if we include financial crimes, then every request will become an urgent and expedited request. I think there is a way, however, to the scenario she described about phishing attacks, for example, could be folded into critical infrastructure which could be expanded to say something like critical infrastructure or online or real-world infrastructure. I would need some wordsmithing help there. But we could expand the word infrastructure to include something like an attack on the DNS. Thanks.

JANIS KARKLINS: Okay, thank you. So, Margie, please think whether you can accept that. Milton, please?

MILTON MUELLER: I was pretty much going to say the same thing that James did. I would just caution us that by creating—and I knew this was going to happen—by creating a category version of requests, there's going to be pressure to inflate it because everybody thinks their request is urgent. I think limiting it to threats to life, bodily injury, and critical infrastructure is unexceptionable. Nobody is going to argue with that. Child exploitation, if indeed that is a threat to some similar kind of real children and not a content-related request, that easily belongs in there.

I would just inform James that DNS is already defined as a critical infrastructure in most Internet circles, so I'm not sure we even need to specify that. But if you think it helps, I'd be okay with that.

JANIS KARKLINS: Okay, thank you. So then we could put maybe in the brackets after critical infrastructure, online and real world. Something like that. James?

JAMES BLADEL: Thanks, Janis. I take your point, Milton, and we can make that language however it needs to read so that everybody is happy.

I just have a question, really not for Milton or anyone in particular but just for the group. Why are these types of requests not being routed through some law enforcement agency? Is my thinking on this correct, that there is a defined use case for law enforcement but that we're also creating some sort of an urgent request that is accessible to any accredited user or is this reserved for law enforcement? And if so … I'm just trying to understand the overlap here and I would appreciate someone setting me straight on that. Thanks.

JANIS KARKLINS: Thank you. Chris Lewis-Evans?

CHRIS LEWIS-EVANS: Thanks. We had a bit of a discussion on this last week I think. I think the main point here is who makes the decision about what is an urgent request and what isn't? If it's an imminent threat to life, realistically the people that can make that decision and have all the information to make that decision are generally law enforcement, public safety people. So, being able to have an accredited authority that can say that and allow them to make urgent requests in a system would certainly make sense.

But then we come to Margie's point where you may have an attack going on. It's causing massive harm to sometimes very big companies that could have a massive [inaudible]. And the decision there would probably have to lie with data controller. So, I'm just wondering whether this is [inaudible] last week was whether we could separate this off where the decision maker is law enforcement and it's a threat to life type scenario. So, to cover off James, we'd hope that that would get [inaudible] to law enforcement when someone's life is in danger and they are the people that are making the request.

Then, where it is posing a critical infrastructure type aspect, that the decision maker might then [inaudible] to the deciding body, so you have to provide that [inaudible] why you want the urgent request.

So, I'm just wondering if we can split these two a little bit where that decision around the urgent request gets made. I think that might make our life a little bit easier. Thanks.

JANIS KARKLINS: Okay. Let me take Greg.

GREG SHATAN: Thank you. We've talked about before how mitigation and the functioning of services on the Internet are not looked after by law enforcement. They're looked after by the entities who are either providing security or providing the services.

As an example, let's say the DNS of a major hosting company went offline because it was being attacked. That can disrupt the resolution of email and website for significant portions of the Internet. Law enforcement's job is not to deal with mitigation in that case and solve the problem. You're going to get a call from the company that's being attacked or people working on its behalf.

Now, I would argue that such incidents are high priority because they affect millions of people. And these happen occasionally. So, it's not just an issue for law enforcement. And there would have to be some judgment and justification about why an incident like that is going to be an important high priority one.

So, to answer James's question, no, this isn't just law enforcement. GoDaddy itself, for example, is an example of a company that if it was affected, millions of people would be severely impacted. Thanks.

JANIS KARKLINS: Thank you. Margie?

MARGIE MILAM: I was going to say the same thing that Greg said, that law enforcement obviously has a role but a lot of large corporations that provide Internet services or online services are doing this day in and day out and sometimes they work with law enforcement, sometimes they don't, but they do what they need to in a very quick timeframe to resolve issues for their customers.

JANIS KARKLINS: Yeah. Look, also we need to always keep in mind that we're here talking and trying to define a policy. As such, our look to issues need to be maybe not that granule but more holistic. So far, what I heard, I think the current text represents all these cases, even if it is not prescriptive, whether we're talking about law enforcement or any other requestor. But let me take Frank followed by Mark SV.

FRANK CONA: So, for the record, not a question I'm raising. I really agree strongly with Greg, as I said in the chat. A lot of issues will be dealt with by the private sector, not because they're less important and not important enough for law enforcement. They may be major. But their technical nature will mean that private sector, not necessarily industry, entities will be the first to respond.

Point two. We can have … So, just to be clear. We're not talking about financial crime. We're talking about financial harm. So, not financial crime, just financial account hijacking or insider trading or something like that. We can have financial harm. You can make harms that are fairly considerable. Either they affect a large population or they affect a smaller set of entities, individuals, but in a very acute way and to think that those can just be dealt with in a much lower fashion is just going to be an untenable position. Those make the headlines every day.

JANIS KARKLINS: Thank you, Frank. Mark SV, Volker, and I would like really to draw the line on commentaries. Mark SV, please.

MARK SVANCAREK: Look, the reason that we're debating E and talking about a separate accelerated timeline is because on the regular timeline we're being told that people are going to ignore us on weekends and holidays and things like that, that this will not be treated the same way as the abuse contact line which I think is 24/7. We're being told pretty clearly for a long period of time that the normal timeline is going to be kind of whatever. So, that's why there's this strong urge to create an accelerated timeline. If we had some sort of confidence or assurance from this group that we would be working to develop a real timeline, a standard timeline, that didn't require so much expediting and urgent cases, then it wouldn't be so critical to us to have to come up with a separate E and argue about what's urgent and what's not.

So, I think we're focusing on the wrong thing. If the normal timeline is just sort of a whatever timeline and there's no expectation that it will be reasonable to us at all, then we have to create this separate category. And I agree with some people who said if we call it urgent, then people will want everything to be urgent. But that's just because the non-urgent category, we're being told that that's not really a priority for anybody else. So, that's where the concern is coming from. And I think if we acknowledge that and address that in our normal timeline, then E becomes a lot less of a problem for everybody. Thanks.

JANIS KARKLINS: Yeah. Thank you, Mark. I think we should not be that [emotional]. We had a conversation. There is a proposal. We will come back to that proposal which is the last sentence of sub-point C. But I simply want to go through the whole text before coming back to those points that we have examined during the previous call. Volker, please.

VOLKER GREIMANN: Thank you, Janis. I don't think that Greg's argument holds water. Well, maybe like a leaky bucket but not very much further. Since we are talking about WHOIS data here or what used to be WHOIS data—so, registration data—I fail to see how any third-party abuse handling company is able to use WHOIS data, just how it can be that urgent that they cannot use the normal channels.

I mean, law enforcement, I understand. They have means to act up on that data stat and take action and make sure that the significant harms that they are fighting are taken care of. But third parties have no jurisdictional powers, have no ability to act upon that data in a legal fashion. So, having that data or not having that data can't be that urgent.

And as Mark said, it sounds like it's just a round about way to speed up your normal requests by expanding the urgent category as far out as possible. I think e should allow the kind of requests that the urgent category is intended to deal with to function. We need to make sure that only the most urgent, the most narrowly defined requests can fit in that category. Otherwise, that category will be just as full as any other category and will just quickly turn into the same kind of response times that the normal requests get.

So, I fail to see the argument and I think we should define this as narrowly as possible, just to maintain the usefulness of that urgent contact as well.

JANIS KARKLINS: Thank you. So, as Caitlin mentioned in the chat, the definition and the rest of those urgent requests have been drawn from the implementation document. If you could specifically, Caitlin, put the reference to that document, that maybe will be helpful. So, this is rather clear, at least to me. Let me take Milton, Greg.

MILTON MUELLER: Hello. So, let's give Mark a break. I think it's a valid thing to say that since we're not making firm commitments for normal requests that we should have an urgent category. But again, by that very same token, we need to strictly limit and precisely define the things that go into that. And you can expect us to completely resist any attempt to expand it to things like financial harm which could mean millions of people in millions of incidents every day. I think you're just going to have to accept these very clearly defined sets of conditions as to what constitutes an urgent request and I don't think we should be spending that much time on this.

JANIS KARKLINS: Thank you, Milton. I'm trying to close the debate but the debate is going on. Greg, please.

GREG SHATAN: I'm going to respond to something Volker said which was making a request doesn't have really an effect and isn't useful. I've been involved in some responses to some pretty serious problems in which we had to figure out additional domains involved in attacks. And those were very timely operations. The effects of the activity were really significant on a variety of users.

We have a group here that has expertise and what I'm not hearing people do is ask questions sometimes. What I'm hearing is people speaking authoritatively about things sometimes they don't have a lot of background about. That's what Volker did. We can do better than that. Thank you.

JANIS KARKLINS: Thank you, Greg. Mark?

MARK SVANCAREK: Sorry, old hand.

JANIS KARKLINS: James?

JAMES BLADEL: Thanks, Janis. I actually wanted to respond to Mark SV's previous intervention because I think I may have an answer. I apologize, Mark, if you felt that I was cherry picking your intervention. I really thought I was responding to the heart of your concern. But I think I have a way that we can capture, or let's say maintain the value of bullet point E so we don't have to throw it overboard because that's kind of where I was trending five minutes ago. But instead we can preserve it as long as we capture this idea that the output of or the result of a request that is submitted through this urgent channel could be obviously disclosure of the private data or if the data controller were to say, "We don't believe that this qualifies as an urgent request," and refers it back to the normal channel, to me that would act as a trap door to capture some of the frivolous or potentially duplicative request and the abuse of this emergency channel.

Essentially, it would be like a 911 operator saying, "You got a cat stuck in the tree. Please call the regular number. Don't call 911 with this kind of stuff." As long as the data controller had the discretion to bounce these things back out of the urgent channel and into the normal channel, I think I could live with E. Thank you.

JANIS KARKLINS: Thank you, James. After listening to all these arguments back and forth and adding critical infrastructure in brackets online and maybe offline, can we stabilize this text? Any objections? Can I ask to put in brackets after critical infrastructure in real time? Online and offline. Probably that's the most useful jargon.

UNIDENTIFIED MALE: Just a quick observation. Wouldn't we want to say that they are threat to the functioning of critical infrastructure or is that implicit? Maybe we don't need that but something to consider.

JANIS KARKLINS: There is a threat to critical infrastructure means also the functioning of critical infrastructure. I think this is simply … Again, this is drawn from other documents that have been already used, the same formulation and the same category. So there is certain unification in that respect. I hope it is acceptable now. Frank?

FRANK CONA: I mean, I think the grammar here in E may need a little bit of clean-up. I'm not entirely clear. Does imminent threat refer to everything that follows, to life, to serious bodily harm, to critical infrastructure? Is that the case?

JANIS KARKLINS: Yes, it is.

FRANK CONA: So, it's an imminent threat of serious bodily injury. So, if there is a threat of serious bodily injury that isn't imminent … I don't know.

JANIS KARKLINS: I understand. The whole of my previous experience in 30 years suggests that dealing with these types of things we would get into 2025 to finalize the document and I would like to ask whether this is something that you would kill me if that would stay in the text. If you would not, then let's stabilize it and fine-tuning and polishing of the text we can do when we will do the final reading because certainly there will be some things that need to be aligned, rephrased, without changing context simply to make text flow and so on, and that would be then time to do these types of nail polishing things. If you would accept, Frank.

FRANK CONA: Yeah, go ahead.

JANIS KARKLINS: Okay, thank you. Milton, your hand is old, I believe. Thank you. So, then, let's assume that this is something we could live with for the moment and stabilize it and go to the next point.

EPDP team recommends that if the entity disclosing the data determines that disclosure would be [inaudible] of applicable law and result of inconsistency with these policy recommendations, the entity disclosing data must document the rationale and communicate this information to the requestor and ICANN Compliance if requested.

Let me take also next one. If the requestor is of the view that the request was denied erroneously, the complaint should be filed with ICANN Compliance. ICANN Compliance must either compel disclosure or confirm that the denial was appropriate. Alan Woods, please.

ALAN WOODS: Thank you, Janis. Yeah. There's a definite issue here. We are receiving here that ICANN Compliance is competent. Not saying competent in the [inaudible] sense but I mean as the legal sense to decide whether or not the decision to disclose was in line with the law. They are not a competent body to decide that. The only competent body to decide that would be the courts or those who have received delegation in legislation, which again in the European context, would be the data protection commissioners or authorities.

So, the only way that ICANN Compliance can really get involved is if the procedural elements were not held up, not the actual decision-making aspect of.

JANIS KARKLINS: Okay. You have a specific suggestion, editorial suggestion, Alan?

ALAN WOODS: On the fly, no, but we can certainly suggest one.

JANIS KARKLINS: Okay. Hadia, please?

HADIA ELMINIAWI: Thank you, Janis. To Alan's comment, so what's wrong to keep it as it is? If it is not actually within the remit of ICANN Compliance, then ICANN Compliance can tell the requestor that—that they cannot deal with this case and this needs to be dealt with in another way.

JANIS KARKLINS: Thank you, Hadia. My question to Alan before James speaks is if we would take out in violation of … If we would take out "applicable laws and" and the text would remain "in violation of …" So, would result in inconsistency with these policy recommendations. So, we are taking out "violation of applicable law and." Would that be something you could live with, Alan? Because you referred that ICANN Compliance is not competent authority to judge about applicability of law but ICANN Compliance might be competent in judging applicability of policy recommendations.

ALAN WOODS: Thank you, Janis. So, what you're saying makes sense but I've been reminding by my teammate that we actually did propose an edit to this in the actual document, so it is down below. I'm just pasting it into the chat there but it is also in the document.

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

TERRI AGNEW: James, if you're speaking, you may be on mute.

JAMES BLADEL: How about that? I was on mute the whole time.

JANIS KARKLINS: Yeah. Now we hear you. Now we hear you.

JAMES BLADEL: Thanks, Janis. Thanks, Terri, for mute check. I just want to step back for a second and digest what Alan is proposing but I wanted to point out that this section is very concerning for me. It could be the undoing of the entire policy if we create a pathway where complaints about whether or not a disclosing entity made the right legal determination in denying a request, then it's possible that ICANN Compliance could fail and then the entire policy would come tumbling down like a house of cards. So, I just want to emphasize some caution here. Thanks.

JANIS KARKLINS: I'm not sure. What Alan suggests, it is more or less what I said in the chat. If the requestor is of the view that the response from the entity disclosing the data is not consistent with its policy recommendations, complaint should be filed with ICANN Compliance. If a requestor is of the view that response from the entity disclosing the data is not consistent with applicable data protection [inaudible], requestor should contact the relevant data protection authority. Clear-cut description of complaint [inaudible]. Milton?

MILTON MUELLER: Yeah. I have kind of a procedural point here. I just noticed that the Google Doc that is on the screen … So, there was a Google Doc that was circulated by Caitlin yesterday that is the interim report and I've entered comments under that. The Google Doc that's on the screen now is different. Is that correct?

JANIS KARKLINS: Caitlin?

CAITLIN TUBERGEN: That's correct, Janis.

MILTON MUELLER: So, I'm confused about how we're supposed to enter our comments on these materials at this point. Are we commenting on the interim report document or are we commenting on these previously existing building block documents? And if so, what should we be doing with the interim report document?

JANIS KARKLINS: So, methodologically, we're working with the text which is on the screen. The interim report and comments on interim report were solicited in light of developments yesterday. But whatever agreement we will reach on every building block, the initial report file will be adjusted accordingly. Then the comments which are done on the Google Doc on initial report will be considered by support staff once we will get to finalization of initial report for consideration by the group. It is still a work in progress, a document in progress. So, for me, there is no confusion. The text we are working on now are on the screen and the links come from the description of all building blocks and initial report is, for the moment, just supporting document. That's just to give an idea what the initial report could look like once we are done with our conversation.

MILTON MUELLER: Okay. So, then, we've got to back up and rereview these building block documents, in other words. I've got to get the NCSG people to do that.

JANIS KARKLINS: No but these are not new ones. These have been—

MILTON MUELLER: They've been around for a while, okay.

JANIS KARKLINS: Yeah. The building block documents haven't changed and all of them are known.

MILTON MUELLER: Okay.

JANIS KARKLINS: Some edits have been made in initial report, simply because we hope that could demonstrate how much work we still need to do and that we could get through that work in remaining days. So, we decided that we cannot. Now we will go systematically through the [inaudible] building blocks that are published all the time. So then we will import the result of our agreements to the initial document.

So, the text proposed by Alan. Now this has disappeared from my screen. Here it is. Now, what you see on the screen that Berry has highlighted. So, can we replace the whole section … This paragraph that we are talking about which is on the screen in yellow with the one that is now on the screen in blue. If requestor is of the view that response from the entity disclosing data is not consistent with these policy recommendations, complaint should be filed with ICANN Compliance if a requestor is of the view that the response of the entity disclosing the data is not consistent with applicable data protection legislation, the requestor should contact the relevant data protection authority. Very clear-cut and very straightforward. Amr?

AMR ELSADR: Thanks, Janis. I think everything in that text makes sense. I'm a little uneasy with the second half, the part where if the requestor is of the view that the response is inconsistent with applicable data protection law. It's good advice. I'm just not sure how relevant it is to what the GNSO needs to recommend to the ICANN Board. If a requestor is of that view, they can take it up with the data protection authority or they can take it up any way they see fit. I think the bottom line is that the first half of this is what works. If the requestor is of the view that the response from the entity disclosing the data is not consistent with the policy, then they can take that up with ICANN Compliance. Whether it is or isn't consistent with data protection law and who they need to take that up with is probably something that is outside the scope of the GNSO or ICANN.

Like I said, I think it's good advice and we can present it in the form of advice but I don't know if it belongs in a formal GNSO recommendations [of the] ICANN Board and I don't know if it's meaningful at all for the ICANN Board to even adopt this. Thank you.

JANIS KARKLINS: Okay, thank you. You got some support in the chat. So, one option would be simply to limit with the first sentence talking about non-compliance with the policy recommendations. Another option would be to replace “should” with “could” – no, not on this one but in the second sentence. Simply indicating that that would be the part but not any kind of obligation.

Look, let me try with the first suggestion just to keep the first sentence addressing non-compliance with the policy recommendations, the one that now is seen on the screen. But not [inaudible], just this one. So, with this sentence, we would replace—two sentences in the text in yellow on the main screen. That may be a solution. So be it. Thank you. Very pleased. Make necessary changes.

Let me now go to the implementation guidance. Implementation guidance suggests that the entity receiving actual disclosure request must confirm that request is syntactically correct including proper and valid authentication authorization credentials. Should the entity receiving the actual disclosure request establish that the request is syntactically incorrect, the entity receiving the access disclosure request must reply with an error response to the requestor detailing the errors that have been detected. Any issue with this suggestion? Not for the moment.

Sub-point B suggests that should the entity receiving the access disclosure request establish that the request is incomplete, the entity receiving request must reply with an incomplete request response to the requestor detailing which data required by policy is missing, providing an opportunity for the requestor to amend the request. No requests for the floor.

And typically, the acknowledgement response will include the ticket number or unique identifier to allow for future interaction with the SSID. Any issue with this, with implementation guidance?

Okay. So, then we have Marc Anderson which will confirm that there is no issue. Marc, please.

MARC ANDERSON: Hi, Janis. On B, I'm not sure for writing an opportunity for the requestor to amend its response, its request. I'm not sure that necessarily makes sense. We're probably talking about an RDAP type response which is a query and response type system, and there isn't really an opportunity to amend the request. You can submit a new request.

So, I think it would be difficult to actually implement the ability to amend its request. I guess I'm expressing caution about the last part. I think we can probably just drop off "provide an opportunity for the requestor to amend its request." I think that would be fine.

JANIS KARKLINS: Look, we had already this conversation and I do not really want to open it. If we think in practical terms how this request will be submitted, most likely it will be some kind of application with the user interface where necessary data will be typed in, either in an automated way or not automated way. Then probably in some cases there will be multiple choice option where you would click and then choose whatever pre-prepared data should be submitted and then so on.

And then until every field that needs to be filled would not be filled, then the send button would not be activated or active, and only it would turn green only when all data is filled. I think that this will be a real-case scenario how the system will function from users' perspective. So, as a result, incomplete file will not be able to even submit through that type of interaction. But of course I may be wrong. Mark SV, your hand is up.

MARK SVANCAREK: Yes. Thank you, Janis. The reason we need to keep in "providing an opportunity for the requestor to amend its request" is that there is multiple ways that this could be kicked back. So, Marc is talking about the electronic automated part of the RDAP service where maybe it returns a 404 or something like that. And that will just be automatically sent back.

But if there is some question about you did not provide the correct amount of information for this to be a valid request, some element of the payload as opposed to a protocol-level problem, then there is going to need to be a recognition of that sent back and then an opportunity for the requestor to amend that request and send it again without being perceived as being abusive. So, this clause allows us to fix a problem in an on-abusive way. That's why we need to keep that clause in the system. Thank you.

JANIS KARKLINS: Thank you. Marc, would this explanation and what I was trying to say, would you be willing to let it go? Meaning to pass it.

MARK SVANCAREK: Mark SV is willing but I think you're asking Marc Anderson.

JANIS KARKLINS: Yeah, I'm asking Marc Anderson. Sorry.

MARC ANDERSON: I'm going to drop it now. I'm not in agreement, frankly, but I don't see the point in pushing the issue further at this point so I'll let it go so we can move on to other topics.

JANIS KARKLINS: Okay, thank you. Then we for the moment stabilize this implementation guidelines three points and we go now up in the text to a new editorial suggestion that have been made as a result of our previous conversation and see whether this meets the essence of our conversation and captures possible agreement.

So, in sub-point A, we were talking about should the entity receiving the request establishes that the request is incomplete, the entity receiving request must provide an opportunity for the requestor to amend and re-submit its request. EPDP team will further consider whether resubmission of the request will be treated as a new request from the cost and fee perspective. Hadia?

HADIA ELMINIAWI: Thank you, Janis. Just a question. The actual benefit here from amending rather than resubmitting is actually the timing of the response. Correct?

JANIS KARKLINS: There is also some question of fee involved, since we do not have agreement on fee structure.

HADIA ELMINIAWI: Yeah, but if we actually decide on some kind of … So, maybe it's not a new cost. Maybe it's some cost but it's less than the original cost.

JANIS KARKLINS: No. For the moment, we do not know because we—

HADIA ELMINIAWI: Yeah, we do not know. So, there could be some kind of benefit to the cost as well. Maybe yes, maybe not.

JANIS KARKLINS: Yeah. We discussed kind of preliminary that there could be several cost models. One is sort of pay-per-click or pay-per-request. Another model could be subscription cost. This conversation is still ahead of us what type of model we would recommend as a result of our conversation. Let me take Chris.

CHRIS LEWIS-EVANS: Do you hear me?

JANIS KARKLINS: Yes, yes, please go ahead.

CHRIS LEWIS-EVANS: Yeah. My comment is similar. The last sentence [inaudible] doesn't have a [inaudible] response requirement not around any unagreed fee or cost implication. So, I suggest that we just remove that last sentence and that can go in the financial section. I think that's a much better place for it to be. We can talk about repeat requests in any financial model when we get there. Thank you.

JANIS KARKLINS: Okay, thank you. So, please consider Chris's proposal. Laureen?

LAUREEN KAPIN: I'm agreeing with Chris but also pointing out there are really three issues here about the benefits of being able to amend and resubmit. One is timing, two is cost, and three is this risk of being perceived as submitting an abusive request and that's why it's important to keep this language. And I agree with deleting the second sentence.

JANIS KARKLINS: Okay, thank you. Alan Greenberg?

ALAN GREENBERG: Thank you very much. Yes. Certainly, fees should be discussed in the fee section. All of these problems are related and there are situations that occur continually in the real world with customer service requests that there are often to and fro. You come back for more information. And it's handled regularly simply by connecting the request, that when you submit the original one there's an ID number assigned to it. If you have a modification of it, you may be submitting it as a brand-new request but you refer to the previous one. The same can handle fees and things like that. It's standard business that I may have a per-request fee, but if there are iterations that are necessary on it, that doesn't make it a new request with a new fee.

So, I'm not trying to predicate what our fee policy should be but these kinds of things are handled every day in the real world and I don't see why this situation should be any different. Thank you.

JANIS KARKLINS: Thank you, Alan. Look, I think the statement is fairly simple. So, in case of if we allow system to submit incomplete requests, in my mind as I described it, should not be possible simply through the user interface. So then we, as a policy, we say we should allow that this incomplete request, if [identifier] doesn't complete, we should allow possibility to amend. Full stop. So, not to withdraw and formulate completely new request. So, I think it's simply common sense.

BECKY BURR: Hi, Sandy.

SANDY: Hi, Becky. How are you?

JANIS KARKLINS: So, somebody is not on mute and we hear side conversations. Any issue with policy statement, that in case of incomplete request, the entity receiving request must provide opportunity for requestor to amend and resubmit the request? And with the understanding that the fee issue would be described in a fee section as it is suggested now by Berry. Okay. Then we can keep this one as seen on the screen.

And we can move to the next item. This is what we had already—we felt already some tensions in today's conversation. This is about the response time. We had plenty of conversation on this and I think we have here for the moment divergence of opinion how we would formulate this policy recommendation as a result. Based on our conversation last time, we suggest with support staff that for the requests that do not meet the automatic response criteria, a response must be received within the timeframe that is to be determined.

Then, in a footnote, some members of EPDP propose that disclosure response should be returned in one calendar day for urgent requests and preferably within seven calendar days for other requests. Others express concerns about the implementability of—probably there's some word missing—timelines for non-automated requests. The EPDP team will review the timeline further, once it has made a determination on whom will be the authorization provider. So, that is a footnote that we suggest to add explaining that the response time, how we will deal with response time.

So, can we for the moment accept that formulation? And again, this is formulated also in light of initial report. It will not stay in the final report in this format for sure but it reflects the substance of our conversation and it contains the desire of ones and concerns of others. So, no requests for the floor, so I take that the formulation for the moment holds and we can move now to the next building block unless I have omitted something. No, I haven't.

So, let me now suggest to move to building block authorization provider. Authorization provider is the block that we have developed working in a smaller group. Maybe Caitlin can provide with further details.

CAITLIN TUBERGEN: Thank you, Janis. So, just quickly I would add that as we were going through the various models, a couple of EPDP team members noted that we should add an authorization provider building block. So, a small group of volunteers met a few times over the last few weeks and developed this text. And I'll note that a lot of the text had been copied and pasted from other building blocks and put here as a baseline. And you'll not that there are still several comments in the margins but we wanted to put this before the team to see if we could get any agreement or further discussion on the points in the building block. Thank you.

JANIS KARKLINS: Thank you. So, the smaller group worked on the document I think for about four or five hours and this was a group consisting of volunteers. I assume that this might be something which is close to the target, not necessarily 100% on the target but close to the target.

So, method suggested is just to go paragraph by paragraph, and if I may ask not to speak unless you cannot live with the paragraph. With this, is there any chance to get on the screen in more readable colors? Okay. Can we get to the background? Just black and white. That would be easier.

Okay, point one. Authorization provider must review every request on its merits and must not disclose data on the basis of accredited user category alone. For the avoidance of doubt, automated review is not explicitly prohibited where it is being both legally and technically permissible. Any issue with this? I see no requests for the floor.

Let me move to point two. The authorization provider must confirm that all required information, as per building block A, criteria and content request provided, should the authorization provided determine that request is incomplete, authorization provider must reply the requestor with an incomplete request response detailing which requested data is missing and provide an opportunity for requestor to amend the request. This confirmation will also be the responsibility of the central [data] manager if the manager is not the same as the authorization provider. So, this is [inaudible] that we discussed and agreed just ten minutes ago. Any issue with point two? Not for the moment.

Number three. While the requestor will have ability to identify the local basis under which it expects the authorization provider to disclose the data requested, the authorization provider must take the final determination off the appropriate lawful basis. Any issue with this? No requests for the floor.

Authorization provider must log requests, performance the balancing test before processing data where required by applicable law. No issue with this. Alan Woods?

ALAN WOODS: This is an issue but only I suppose in concept. And this is something that we need to think about and this is one of those recommendation calls that we could take a stand on because one of those outstanding issues that we continuously come back to is how are we going to adequately assess [inaudible] geographical location, the data subject [inaudible]. But, also, more importantly, how do we ensure that we're agnostic as to what legislation we are recommending for in this one and what jurisdiction?

I'm just putting this out to the team. This is constantly coming out of the blue for a lot of people. I mentioned this in the small team and I think it's something that is worth [setting] for us, that as the DNS, as the people who are setting a consensus policy for all registrants, we should probably think to almost jurisdictionally agnostic point of view, that if a registrant is being treated as a registrant and equally to other registrants in the review of the release of their data, we should not be penalizing registrants because their own home jurisdiction or country does not have the legislation in place to protect their rights. We should be, again, agnostically looking at this from the point of view of a registrant within the domain name system.

Therefore, on that point, the meaningful human review or the balancing test, for want of a better term, could be a very good basic point for those people within that particular request.

So, instead of that one where we're saying the [formal] balancing test before processing the data where required by applicable law, we could actually make that simpler by just stating that everybody should have a meaningful human review and ensure that the general rights that are set by us in the DNS, either that the policy of the domain name system must be applied in that.

Now, I'm sure, as I said, people will be going head spinning and wondering where that's coming from. But again it's going back to that question I've asked even of myself and in Montreal on a panel was how do we ensure that this is not just GDPR centric? How do we ensure that [inaudible] rights generally across DNS? This is one way that we should possibly think about it.

JANIS KARKLINS: Thank you, Alan, for outlining this issue and [inaudible] this conversation and proposed formulation, again, is attempt to reconcile our task to make a policy recommendation specifically to implement GDPR from one side, but from other side to make this policy flexible enough that if other legislations will kick in, that we need not to review policy as such but simply we extend the level of protection as required by applicable law.

That's, in my view, the proposed formulation is such that would allow exactly the same thing. But of course we may want to spend some time talking through this but always keeping in mind what is our assigned task for this PDP. Alan Greenberg, please.

ALAN GREENBERG: Thank you very much. Janis, I agree with what you said. I think we have no choice but to use words like "under applicable law". If indeed there are other policies and laws like GDPR which have extra territorial capabilities associated with them, then yes, implementing this kind of policy is going to be difficult. Some of us have said from day one we're probably looking at table-driven algorithms that are going to have to factor in these things and that's true whether it's done manually or on an automated basis.

But I don't think we can assume that everyone has protection and therefore we can't give out any information in all of these cases because some law somewhere might forbid it.

As Alan Woods himself has said, that on the requests he's looked at, geographic determination in many cases has allowed him to disclose information. So, I think we need to put that capability in the system.

Now, how a centralized system running at ICANN can make that determination, I don't have a clue, but I don't think we can build it into the policy that we do anything other than follow applicable law. Thank you.

JANIS KARKLINS: Thank you. Amr?

AMR ELSADR: Thanks, Janis. I agree with Alan Woods and I think what we should be trying to do here is seeking to not just limit our policy recommendations to the minimum extent possible of being compliant with data protection law in countries or regions where it exists, but we need to also set a baseline best practices. Alan Woods … Alan. I thought I said that. Sorry. So, I agree with what Alan Woods was saying.

I think we need to also acknowledge that for a very long time ICANN has been not complying with data protection laws and we need to set best practices in our policy recommendations now. We also need to recognize that in a number of different jurisdictions, a lot of these jurisdictions, including in the region where I live in the Arab world a lot of data protection laws are popping up to try to harmonize the way they handle data with the EU's GDPR, and part of the reason for this is because they need to continue doing business with the European Union.

So, I don't think it would be a terribly good idea to differentiate this and say, okay, we recognize that there's data protection regulation in the EU that protects its citizens or people who are physically located there, and it also protects people who use processors and controllers when processing their data. But anyone who is not protected will not be protected by ICANN consensus policies. These people can go ahead and fend for themselves.

Now, in situations where there's an actual conflict with local jurisdictions or local laws, then sure, that's something we might need to address. But it doesn't mean that the baseline recommendations we provide need to necessarily grant registrants or data subjects no protection. Thank you.

JANIS KARKLINS: Okay. Thank you, Amr. Milton, please.

MILTON MUELLER: Yes. I don't know why we're having this debate at all because I need to remind you that ICANN is supposed to be the global governance arrangement for the DNS and if we set a policy that registrants have certain privacy protections, they may indeed be modeled after, or in some way, based on certain jurisdictional laws, but the point is we have [inaudible] supposed to be setting globally consistent policies. If we don't want a globally consistent policy for the DNS, then let's just abandon ICANN and we don't have to do this work and let's have national governments set their own rules and have a completely fragmented DNS. We can decide—and should decide. It is our mission to decide what level of data protection registrants of the WHOIS get.

Now, clearly, we have constraints. We cannot violate jurisdiction-based laws and certain things but the best thing, and the reason ICANN was set up, is for us to have a homogenous and uniform set of requirements for every domain name registrant in the world regarding how their data is treated.

And as Amr said, we can have specific exceptions to that when there's a conflict, but the goal, the whole point of having this multi-stakeholder arrangement is for us to be setting consistent, uniform policies to the DNS. So I certainly hope everybody is on board with that. Heck, if you're not, then let's call it quits and let the legislators and national governments do this work because it isn't that fun, as you may have noticed. Thank you.

JANIS KARKLINS: Thank you, Milton. But can we move closer to the text? I understand that suggestion is to delete "where required by applicable law" right? This is what Amr suggested. If that is true, then let me see whether team can accept this modification. Stephanie is next, followed by Margie.

STEPHANIE PERRIN: Thank you. I don't want to repeat what Alan and Milton have said. I agree with them, Alan Woods that is. I would just like to point out that in addition to the fact that we are providing a uniform policy that basically reverses the prior uniform policy which said disclose all data and forced registrars and registries to use the conflicts with law procedure if they wished to comply with data protection law. We are now reversing that and coming up with a uniform policy. And if there are those rare instances where law is in conflict with a general harmonized policy to protect registrant rights, then perhaps subsequent PDPs can revisit the conflicts with law procedure to deal with those exceptions.

But I'm a little out of date with our colleague In Australia, [Green Leaf], latest update. It's well over 120 laws now and they are all, as with the European directive previously, trying to achieve a GDPR-like standard. So, it would be foolish and very expensive to attempt to come up with a policy that actually reflected each different law. We have to go with a uniform policy. Thank you.

JANIS KARKLINS: Thank you, Stephanie. Margie?

MARGIE MILAM: I disagree with the deletion of that language. I think where we disagree with the statements that were made previously is that the policy that we have developed here goes beyond GDPR. Example, we're redacting legal persons, we're redacting city fields. So, where I think that there's a disagreement is that there could be no need for manual intervention for every single lookup when you're dealing with, for example, a legal person. That might be an automated disclosure processing where a balancing test is not necessary. There's also other legal bases that could apply beyond 61(f) and essentially implies that the balancing test applies even if 61(f) doesn't apply.

So, I think that's a problem and that's the reason we talked quite extensively in the sub-team about it. I think that moving some of that now would be problematic.

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

AMR ELSADR: Thanks, Janis. I very much agree with what Milton and Stephanie were saying and I just wanted to add another quick point. If we recommend that ICANN adopt a consensus policy that is not uniform across all its contracted parties, then effectively we are encouraging ICANN to differentiate between its contracted parties' ability to act in the marketplace.

So, if you live in a country where you don't have the data protection laws that the European Union, for example, has, then basically we're telling people in that country to go ahead and register all their domain names in the European Union and abandon ones that may exist locally.

I don't think this is a healthy policy recommendation for us to be making and I wouldn't imagine that ICANN would want to create that kind of differentiation in its consensus policies either. Thank you.

JANIS KARKLINS: Thank you. I will take Mark SV and Hadia and then I will try to make a proposal. Mark SV, please.

MARK SVANCAREK: Thanks. The previous language worked for me because, for starters, it just says a balancing test. It doesn’t say GDPR. Does someone have a ….? I’ll try again. It doesn’t’ say a GDPR 61(f) balancing test. It just says a balancing test.

Secondly, we know that there are other circumstances where a 61(f) type balancing test would not be required. We’ve already established there’s multiple bases for doing the processing.

So, I think we have to keep the existing language. I think the first clause is generic enough to work without falling into this rhetoric that some people have rights and some people don’t. And secondly, the second clause is required because there are certain circumstances where it will be clear that a 61(f) balancing test is not going to be required. Thanks.

JANIS KARKLINS: Thank you, Mark. Now, Hadia, you wanted to speak. Your had was up.

HADIA ELMINIAWI: Yes. It’s just that I wanted to note that [inaudible] balancing test before processing the data where required by applicable law. Actually, if we deleted the balancing test as not always required, as others said, and it’s only implied under 61(f). But under certain situations also under 61(f) it might not be required. We don't know yet.

I don't know why from the start we need to tell the authorization provider that you will need to performing a balancing test. Supposedly, the authorization provider doing this job will be following GDPR and the rules and does not need us as an EPDP team to tell them, "Look, you need to perform a balancing test," if it is required.

If it iso, and we need to state this, we need also to state that everything else that's mentioned in GDPR with regard to the disclosure of the data.

So, honestly speaking, I don't see the need for us to determine the legal requirements for an authorization provider or what he actually needs to follow, to comply with GDPR. Thank you.

JANIS KARKLINS: So, I was planning to propose something to reflect the notion of the same policy should be applied to all data subjects but I see that Milton has proposed elegant way forward, to replace "where required by applicable law" to replace "where required by policy." He got some kudos from other team members. I see a new hand from Laureen and I believe that Stephanie's hand is old. Laureen, please.

LAUREEN KAPIN: I'm just wondering, for Milton's suggestion, if that's not a big circular because I think some of the concerns that were expressed are that the policy is going beyond what GDPR requires which is the primary law that we're dealing with, although we do want it to have enough flexibility to deal with others. So, just by saying "where required by applicable policy" I don't know where that gets us because isn't that exactly what we're debating, what the policy should be? At least with restriction of applicable law, then if a balancing test is not required, one doesn't have to do one. And I think that's the whole point here. So, I don't see where something [inaudible] to required by policy gets us anywhere because we're still debating what the policy should be.

JANIS KARKLINS: Okay. Alan Greenberg?

ALAN GREENBERG: Thank you. Basically, I was going to point out this is circular unless Milton has some other policy discussion that we're going to have which is going to refine the policy even more. To simply say the policy says it's determined by policy is a completely circular argument.

We're implementing GDPR and other regulations. We cannot set our own rules that are necessarily different from other things. That's not the business we're here for. We have been reminded continually that we're here to implement GDPR and policy regulations to make sure that our contracted parties can operate in these environments, not to create law upon ourselves. Thank you.

JANIS KARKLINS: So, maybe Milton can [inaudible] on his proposal.

MILTON MUELLER: Yes. I think it's quite clear … I mean, to say that it's circular is not necessarily true. In fact, the policy can indeed specify later where we think a balancing test should take place and that would be very easy to do. We could just put in something similar to what we have already tried to do.

But let me just clarify what we are doing here. I was very surprised by Alan's claim that this is not what we're here to do. We are not here to implement the GDPR. We were told by the post-GDPR world that WHOIS is going to violate the law because it doesn't protect the privacy of registrants.

What we are here doing is protecting the privacy of registrants, the private data of registrants, and we're in some sense GDPR is a minimum baseline that we have to conform to in order to be compliant with a very large part of the world. But there's nothing stopping us—and indeed it is our obligation as policy makers for the DNS—to create a globally uniform policy that applies everywhere, particularly since the laws in the world are going to be changing constantly as we go forward.

So, our minimum requirement is to note violate GDPR but we are, in effect, setting a privacy standard for WHOIS registration data. That's what we're doing and that is a policy matter, not simply a matter of applying applicable law, which again sends us into the garden of weeds and nettles of fragmented jurisdiction and discrimination among registrars and registrants. So, I don't think this is problematic at all. I think it actually greatly simplifies our task.

JANIS KARKLINS: Okay. let me give a shot. Based on what we discussed, the policy should not be selective and should apply to all data subjects or registrants. And in the context of our conversation here, the authorization provider must—and we are talking about perform balancing test before processing data where required by applicable law, as suggested by a small group, indicating by Alan, that there may be different regimes and that personal data should be protected in the same manner.

So, what if we would replace this bullet—entire bullet—with the following statement, policy statement. Authorization provider must apply this policy in harmonized manner to all registrants or with regard to all registrants. So, I think that this represents the conversation that we had and I didn't hear anyone contesting that personal data should not be protected as a matter of policy. So, let me [inaudible]. Can we get that text on the screen by any chance? Apply this yesterday in harmonized manner to all registrants. In a harmonized manner, in the same manner. Apply this policy in a harmonized manner, in the same manner, to all registrants [inaudible]. So, this is the proposal. Let me take … Stephanie, is that an old hand or new hand?

STEPHANIE PERRIN: Thank you, Janis. I agree with your text. It is a new hand. I just wanted to respond to this to kind of explain what a harmonized policy is. You select a modality of interpreting data protection law that is at the highest or high standard. And this has happened in firms that have international staff and moved them around. They've been following for HR data protection for their employees the EU law for decades now because it saves money and hassle and is impossible to move people around if you have different regimes under which their data has been collected and protected. It's common sense.

Now, I'm well aware that jurisdiction picking is the game du jour. You establish in Ireland because they've got weak data protection. Sorry, Alan. You incorporate somewhere different where they have no protection for employees. We're all well aware of that. Tax havens and all the rest of it.

But if we want a system that works, we have to harmonize. We have to select modalities. By modalities, I mean things like the balancing test. It's a sensible way of doing data protection law. Every jurisdiction is figuring out whether their law meets the balancing test standard. I just spent two hours with our experts on our recommendations to our government on upgrading to GDPR compliance. This is just what happens. So, it's perfectly normal for us to be doing this. Thank you.

JANIS KARKLINS: Thank you, Stephanie. I would like to remind that we have three minutes to go. Margie, please. Margie?

MARGIE MILAM: This whole discussion of geographic distinction and how to harmonize I think deserves a separate conversation in a separate section. I don't think this is the place for it. If I could remind everyone how we got here, this language originally was meant to track the process steps that Alan Woods had basically shared and it was very helpful on how he does his thinking on doing the balancing test.

And if you recall, when Alan talked about it, he mentioned the fact that he actually does look at the geography of the registrant in determining the risk level.

So, I think this is not the right place to have this. I think we need to have this discussion and maybe create a separate building block for it. It may even be a priority two discussion that we have to get to. But my suggestion is to not include that in here and to save that concept for a further discussion.

JANIS KARKLINS: Okay, thank you. Alan Greenberg, you are the last one.

ALAN GREENBERG: Thank you very much. I'm afraid these words are just too general and subject to multiple interpretations. As Margie made reference to, Alan Woods had said that he's never actually had to perform a balance test because things like recognition that it was a legal entity and not subject to protection. To simply say you're going to protect everything without necessarily considering these uniformly I don't think is appropriate. Thank you.

JANIS KARKLINS: Okay, thank you. So, let me then conclude with the following. Point four for the moment sounds the authorization provider must log requests, full stop. We take an action point that geographic application of policy will be discussed separately. By this, I would like to close discussion on point four and tomorrow when we will resume our meeting we will start with point five. And with the staff, we will think what is the most appropriate place to discuss this geographic applicability of policy.

So, with this, I would like to thank all team members for active participation in today's meeting. So, you saw that time flies faster than we want and even we decided to move the publication of initial report after or as a result of the face-to-face meeting. We still need to proceed swiftly in our discussions and the best way of doing it is to prepare conversations and provide comments undiscussed or documents that we will be discussing in writing that we can take all comments already into account and maybe even modify text as a result based on those comments before the meeting that would curtail conversation and bring us closer to consensus.

So, with this, thank you very much. We are meeting in 22 hours from now, tomorrow at 2:00 PM UTC. Thank you very much. This meeting stands adjourned.

UNIDENTIFIED FEMALE: Thank you, everyone. Once again, the meeting has been adjourned. Please remember to disconnect all remaining lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]