ICANN Transcription
GNSO GDPR Q&A Session with the GNSO Temp Spec gTLD RD EPDP Team
Wednesday 19, September 2018 at 1300 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. The audio is also available at: https://audio.icann.org/gnso/gnso-gdpr-epdp-gtld-rd-temp-specs-19sep18-en.mp3

Adobe Connect Recording: https://participate.icann.org/p2ay385gtib/

Attendance is on the wiki page: https://community.icann.org/x/lAWrBQ

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page: https://gnso.icann.org/en/group-activities/calendar

Coordinator: Excuse me. Recording has started.

Terri Agnew: Thank you. Good morning, good afternoon and good evening and welcome to the GDPR Q&A Session with the EPDP Team meeting and Becky Burr taking place on Wednesday, the 19th of September, 2018 at 1300 UTC for two hours.

In the interest of time, there will be no roll call. Attendance will be taken via the Adobe Connect room. If you're only on the telephone bridge could you please let yourself be known now? Hearing no one, we have listed apologies from Ayden Férdeline, NCSG, and Emily Taylor. Ayden has formally assigned Tatiana Tropina as alternate for this call and any remaining days of absence.

During this period, the members will have only read-only rights and no access to conference calls. Their alternates will have posting rights and access to

conference calls until the member's return date. As a reminder, the alternate assignment must be formalized by the way a Google assignment form and the link is available in the agenda pod to your right.

Statements of interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now. Seeing or hearing no one, if you need assistance updating your statement of interest please email the GNSO Secretariat.

All documents and information can be found on the EPDP wiki space and there is an audiocast and view-only Adobe Connect room for nonmembers to follow the call. So please remember to state your name before speaking. Recordings will be circulated to the mailing list and posted on the GNSO calendar for this – the GNSO calendar for this meeting. With this I'd now like to turn it back over to our Chair, Kurt Pritz. Please begin.

Kurt Pritz: Thanks very much, Terri. And thanks, everyone, for the on-time start. I just want to welcome and thank Becky for making her time and expertise available today. Many of you know Becky's a member of the ICANN Board but I also am pretty sure most of you know Becky was sitting at the table for the start of ICANN, took part in the initial discussions around many of the very first policies that gave ICANN its value to the domain name space, was there for all the gTLD rounds, helping with the 2000 round, an active participant in the 2003 round and then, you know, helping us through many of the advances ICANN made in the growth of ICANN.

And as you know, lately she's the Board leader in this subject matter and not only participates in ICANN on this subject but globally in many different fora. So, Becky, I haven't seen you for a while but thank you very much for coming and please conduct the session the way you see fit and I'm sure the group will have questions, so it's good to hear your voice.

Becky Burr: Thank you so much, Kurt. And good morning from Washington DC, good afternoon, etcetera, to everybody who's here. When I was first asked to do this, I had the good sense to know that this falls into the category of absolutely no good deed goes unpunished. But I decide that I would say yes in the notion that if I could help out at all I was happy to. And I was sure that 27 people would object to my doing it because I'm on the Board or I'm not a European lawyer or I work for a registry. So I'm sort of – I don't even know what to say, apparently nobody objected.

What I'm – for very high level brief introductory slides which are really meant I think to sort of capture the – why this is hard. And then I know that you have many questions, I've seen some of them so I propose to move right into questions from that. Let me just say that I have to say or sort of my own view, they are not the words, views, they haven't been endorsed by the Board or by – or I'm not aware that I disagree with Org on any particular issue but I just want to be clear, I'm doing this here to sort of generate a, you know, add a perspective and some data into the discussions and to help in any way I can.

One of the reasons that we find ourselves in such a difficult place and I know that this is particularly difficult for the lawyers who want to sort of revert to black letter law, is with GDPR is principle-based. It incorporates privacy by design principles, which tell you how to think about privacy and how to consider privacy as you go through your data processing activities, and also is very much hinged on fair information practices principles.

Those are principles that provide guidance but they are not prescriptive in the sense that they do not say, "You may not collect information for the following purposes," or, I mean, they do in some cases but basically they are not prescriptive, they're principle, it is principle-based and it's not possible to know with certainty in advance how the critical balancing test that apply in the ICANN environment will be applied.

And we have to acknowledge that notwithstanding the efforts to harmonize it's entirely possible that those tests will be applied in a different way from member state to member state. Now hopefully, over time, that – those differences will resolve. But at the moment we really are in a state where we don't have clear guidance and it doesn't appear that we're going to get clear guidance in the short term. ICANN is working very hard to clarify the legal guidance but in the meantime we are working with on a more difficult basis.

Fundamentally you have to have a legal basis for processing personal data under GDPR. And there are a couple of lawful bases that are relevant to ICANN but for reasons that I'll talk about very briefly, are more or less difficult to apply. So, the ones that are really, you know, that we need to think about are – that you can process data with the consent of the data subject; you can process data in the public interest and you can process data to further a legitimate purpose consistent with privacy interest to data subjects.

Now, we're going to talk about the limitations on those so those of you who are GDPR experts, I know I can hear you screaming and groaning about whether they're relevant to ICANN, and I think that's a good question. But the point I wanted to make here is even where the processing is lawful, you still have to have adequate safeguards in place and the data minimization principle has to be respected. So it's not just enough to say there a lawful basis for it therefore all things can happen; it really requires us to think about sort of what's the lawful basis, who is entitled to process data on that basis and what safeguards must be in place when they do that.

So the – really – and I know all of you know that, in many ways we come down to the legitimate interest test at ICANN. Consent is a lawful basis for processing but it must be revocable and real and informed, an individual must be able to withdraw that consent at any time without significant consequences. That makes reliance on consent extremely difficult in the ICANN environment.

There also is a public interest derogation where processing is necessary for performance of a task carried out in the public interest or in the exercise of official authority. Now, ICANN as we all know, is required by its bylaws to operate in the global public interest and our policy development process is specifically defined in the bylaws as the mechanism through which we identify the global public interest.

The problem is that under GDPR, global public – public interest authorization basis really needs to be laid down in either European or member state law. And that's why, for example, you can have laws such as I believe Finland has a law that specifies what data has to be made public. There is a regulation that is applicable to dotEU and that lays down certain requirements with respect to GDPR. But those are not generally applicable outside of the context in which they're written.

I think it's probably safe to say that if you're processing data about a Finnish individual, the Finnish data protection authorities and you follow the prescription set out in the Finnish law, the Finnish data protection authority is not likely to come after you, but it's not an – it's not an entirely clear thing. And so we don't have – ICANN is not – does not create European or EU member state law or regulations.

So again, notwithstanding the fact that we are being urged over and over again by many parts of the community to make sure that we are reflecting the public interest in accessible Whois as a matter of law it's very difficult to rely on that lawful basis. And, you know, thinking about how to address that is one of the ways ultimately that we could resolve this issue.

So what it comes down to us is the – where the processing is necessary for the purposes of the legitimate interest of a data processor where those interests are proportionate and respectful of the privacy rights of the individual. So here's what I do when I'm thinking about the legitimate interest

test is to, you know, to start with the personal data elements that are collected to run DNS and to achieve ICANN's purposes.

And then understand who, what, why, the context in which those data elements may be used by a third party for a legitimate interest. And just to understand why this is so hard is that context is critical so, you know, high level blanket statements are very hard to get very comfortable about, yes, a, you know, processing in pursuit of X worthy goal is legitimate and in the – and, you know, legitimate interest and proportionate to the data subject test, well actually you have to now a whole lot of additional information to decide whether you're actually needing that balancing test. Then you have to do the balancing test and then you have to identify the appropriate safeguards.

So in the context of GDPR and the Whois contractual requirements, after a great deal of interaction with the community in consultation with the community input and from the data protection authorities and legal experts, the temporary specification reflects what ICANN Org believes is enforceable in the context of the ICANN environment and your charge here is to take that temporary specification and develop long-lasting policy around it.

Now obviously it – what we have to do is move somewhere within the one-year period allotted to temporary specifications. Does it have to address everything in the universe? Does it have to resolve everything? No, it would be great if it did, but I think what we're seeing in the context of the community discussions regarding unified access or unified access and the manner in which we're using that to seek additional legal clarification there's still a lot of unknowns out there that need to be addressed.

So I just wanted to sort of kind of pose the problem and then let's go ahead and turn to questions. And I don't know – I got some questions, so, Kurt, tell me if you want me just to sort of march through the questions or if you think people should be – just go ahead and ask them. What do you want to do?

Kurt Pritz: Well I think you could probably manage the queue better than I, so I would use the questions that people took the time to submit and sort of march through them, but keep an eye on the queue. So…

Becky Burr: Okay.

Kurt Pritz: You can move back and forth in your own judgment.

Becky Burr: Okay. Let me just start with the question about the difference between a purpose and a legitimate interest. And I think purpose is just a statement of why you are processing data. I'm processing data to identify and respond to instances of fraud. I'm processing data to – for marketing. I'm processing data for the purpose of providing a service. I'm processing data to comply with law. Those are purposes in and of itself there are million, you know, there are obviously an endless supply of reasons that you might want to process personal data.

A legitimate interest is what gives you the – a legitimate and proportionate interest is what gives you the lawful basis under GDPR. So it's not enough simply to say you have a purpose, you must look at that purpose and then determine whether you have a legitimate interest in the processing. And that, again, comes with the requirements for balancing and consideration about whether reasonable safeguards and appropriate safeguards are in place for this.

And then I'll just go on and then I'll go to the queue. The difference between ICANN's purposes and the purposes of the contracted parties, so I think if we look at this holistically, obviously registrars collect data to provide the registration service they need information about who is registering the name, they need information and the ability to contact that registrant, an ability to build that registrant and then they need the information about what their name server is and those kinds of things. And they also collect information

about you know, has nothing to do with the list about their interactions with the registrant and all of those things.

So on the one hand registrars have legitimate – a lawful basis because they need to collect this information in order to provide the service. And they may have additional reasons for collecting it. They need to collect some information to enforce their rules and they may need to collect this information to, you know, understand how to make their products better. And those again might be lawful – those might be lawful purposes based on their relationship with the registrant.

Registries obviously need some of that information in order to provide their service and notify – provide the registry service, the registry itself, and they need information in order to enforce their rules, to identify and mitigate against malware abuse, misuse of their systems. They may have other legitimate interests for doing that.

ICANN has a legitimate interest – or ICANN has purposes and I think legitimate interests in collecting the information and using certain information and that relates as the DPAs of the Article 29 Working Party have said, that goes back to ICANN's mission. Now in the case of ICANN's mission, the data protection authorities, the Working Party 29 sort of referred to ICANN's mission at an extremely high level, security and stability. It did not go beyond that in other bylaws which clearly talk about what we mean by stability and security in the ICANN context and which I think permit quite a larger basis for this.

So I think that, you know, there are overlapping and different legitimate purposes but I think ICANN clearly does have a legitimate purpose connected with – associated with fulfilling its mission as that mission is defined and explicated in the bylaws. And I think the correspondence that we've had from the Article 29 Working Party, which was endorsed by the European Data

Protection Board, clearly acknowledges to my mind, a legitimate purpose for ICANN's processing of the data.

I'm going to go to the raised hands here just for a moment, and obviously we have 90 minutes but I hope – there are a lot of questions so I hope we'll be concise in our questions. So first, Kavouss, and then Margie.

Kavouss Arasteh: Hi, Becky. Good morning, good evening, good afternoon, everybody and good day to you. Thank you very much, accepting this tutorial discussion. The question that I have raised, and I have not been answered, there are two terms has been used, legitimate purpose and legitimate interest. Are these two interchangeably could be used and are the same or they are two different things?

And then, who decides that the purpose for which the data is being transferred or want to be transferred is legitimate or not legitimate? And what are the criteria to decide or determine this legitimacy?

Becky Burr: So thanks, Kavouss.

((Crosstalk))

Kavouss Arasteh: Yes, one more question, and not to disturb you anymore. You talk about consent, very good, and you talk that consent may be withdrawn, and that is good. I raise the same question, if I give a consent and I withdraw the consent, first of all, if the withdraw is retractably applicable, that is all information is already sent to be withdrawn immediately? And that happens to those which are already in the pipeline? Thank you.

Becky Burr: Thanks. So just starting with your last question first because I think it's the simplest, basically the bottom line here is consent has to be fully given and totally voluntary if you are relying on consent so that means a person has the

right to change their mind and say, I don't want my data published in Whois or I, you know, whatever.

And the data controllers who manage that have to be able to affect that right. So you can't require people to consent by contract; that's not going to work. As to what happens for data that has been processed subject to somebody's consent that is withdrawn, that's not entirely clear to me. But I don't think that it's enormously practical to impose this in a cascading way.

But what I will say is that in the – it's very clear that if you are a controller and you are processing data on the basis and you engage in (onward) transfers of that data to third parties, if a data subject comes to you and requests that – and withdraws consent and requests that data be erased or those kinds of things, you as the controller do have an obligation to make an effort to communicate and affect that consent with third parties with whom you have shared the data. So that's a – that's – that I know. I'm not sure how it would work in this context but I can tell you how it works in the marketing context.

With respect to legitimate – with respect to purposes and legitimate interests, the GDPR generally uses the word "purpose" as a standalone. There are a couple of places where I've seen "legitimate purpose" but generally a purpose is a purpose, it's here's why I'm – somebody's going to make us all sea sick with rotating the slides here – a purpose is a purpose, I want to do this for marketing; I want to do this to protect – to investigate misuse of my trademark, I want to process data to protect consumers, I want to process data to sell my goods and services.

Those are all purposes, they are not necessarily legitimate interests because in order to be a legitimate interest, which then has – provides a lawful basis for processing under GDPR, it has to be – it has to be balanced and proportionate with the privacy rights of the individual and sufficient safeguards have to have been taken to make sure that the rights of the individual data subject are going to be respected.

So I think you know, the lawful basis is tied to a legitimate interest which involves the balancing test and the safeguards of purpose, I think is best used as just a description of what's the reason I would like to process the data. Margie.

Margie Milam: Thanks, Becky. And we've been talking about a lot of these things on our call. One of the things that you didn't touch upon is other bases under GDPR that could apply. So for example, say Article say 6(b) related to the performance of contract, that particular lawful basis for processing under GDPR doesn't have the balancing test that applies in the one that relates to legitimate interest so if you look at 6(f), that's where you see the balancing test that's been incorporated into the temporary spec.

So my question really is, and then there's also obviously the consent, there's processing necessary to comply with the legal obligation that the controller is subject to. So there are other sections under GDPR that apply to the data we're talking about. And I don't know if you have any insight into why the temporary spec only focused on the legitimate interest one as opposed to the other ones but that certainly come up in our conversations.

And in particular, it matters when you get to, for example, the UDRP and how the UDRP might be applied because the UDRP and the URS are things that the registrant consents to actually in the registration agreement itself. And so in order to effectuate those dispute resolutions you need to be able to provide the information, you know, and have that information provided for the purposes of that arbitration proceeding. And so I'm just curious how, you know, your thoughts on the performance of contract aspects and whether the balancing test applies to those.

Becky Burr: So I think a good question. I think that that when you're looking at necessary to fulfill a contract, you're talking about the relationship really between registrants and registrars because registrants generally don't have

contractual relations, well sometimes they do have some minimal contractual relations pass through registrars – with registries but they don't have a contractual relationship with ICANN. So it is hard for ICANN to invoke necessary to perform a contract as a lawful basis for processing here.

And I believe that was specifically addressed in one of the letters that we – one of the communications that we received from the data – from the Article 29 Working Party. I think that in terms of the contract you've agreed to comply with a dispute resolution, I would say that probably is a lawful basis. The question would be what are the circumstances under which that data is made available in the context of UDRP for example.

But I think that the – so I think necessary to fulfill a contract may have – may have a place in the relationship between a registrar and a registrant but it is very difficult for ICANN to invoke that as a legitimate basis – as a lawful basis.

Margie Milam: And part of what we're doing in this group is identifying each subset of users and parties I guess, and identify where the purpose lies. And so but do you have any insight as to why the temporary spec did not include some of the other bases that, you know, could potentially apply?

Becky Burr: Well I mean, if there's anything other than necessary to perform a contract, that you're thinking about?

Margie Milam: Well consent is obviously one, right? And I understand that there are difficulties in getting consent but it's not impossible. And so one of the things I think would be useful from – to hear from you is the elements of, you know, that could apply to getting consent because I think that's an important basis to keep in mind and to see whether it can fit into the policy.

Becky Burr: So, I mean, I think that consent could fit into the policy. It was certainly not something that, you know, that there are not really systems set up right now

by registries and registrars to, you know, to affect consent; there are limits to it. You have to know who you're getting consent from and what they are entitled to consent to. So, for example a registrant couldn't probably consent to having a different admin or tech contact personal data disclosed or at least it would be extremely difficult to rely on that.

But, you know, consent could be worked into an ultimate policy knowing however that it is going to require systems to be built in particular ways that they do not operate right now. So I think the judgment was at the time, that that was not a practical – that was not a practical basis for – it was not practically useful as a lawful basis.

And then with respect to necessary to fulfill a contract, I think that the view is that legitimate interest in terms of UDRP is also, you know, better describes what ICANN's lawful basis at that – for requiring that data to be made available in connection with a UDRP.

Margie Milam: Well we don't have a legal opinion on that thought, right?

Becky Burr: Not that I'm aware of. I mean, you know, no, not that I'm aware of.

Margie Milam: Okay, yes, it's just – this is all principle-based so as you mentioned earlier, it's hard to identify where to, you know, how these are applied. So well thank you. I think those are my questions.

Becky Burr: Okay. I'm seeing some questions appear in the notes and action items are those questions that I should go to, Kurt? Or should I just continue marching through this list that you sent me?

Kurt Pritz: Yes, I think the list that was sent to you were people that took time to send questions ahead of time so we should – I think we should look at those.

Becky Burr: Okay.

Marika Konings: Yes, and this is Marika. Sorry, Becky. Just to clarify that the questions on the right, the first ones of those should already be the ones that you have on your list as well. And we had some people adding questions I think after we sent you the questions so once you get through your list I think if you then scroll down to the note pod you'll probably find some new questions that weren't on the list that we sent you, so if there's time left there are some additional one that you can hopefully address.

Becky Burr: Okay. So I think I've talked about how the legitimate interest that relates to disclosure and access might differ between ICANN and the contracted parties. And the answer is, you know, they're different depending on the role that you're playing but also there are probably some overlaps here. Transparency requirements of the GDPR, obviously one of the fair information practices principles is that you process personal data in a way that is fair and transparent, that you describe what data you're processing and the purposes for which you are processing it, and that you make that information available to data subjects.

We obviously do have some requirements existing in the contract regarding disclosures about the use of Whois data. And I think that the, you know, the transparency issues are, you know, we do have to have a clear statement about what data is being collected and why it's being collected, with – for what purpose it is being collected and processed and with whom it's being shared for what purposes.

Data minimization and necessity, how do they apply to registration data, well I think that the, you know, data minimization is an overarching principle, so when you collect data you have to have a lawful basis for it. Here we're talking about – let's say either providing the service in the case of a registrar, that's fairly straightforward, legitimate interest in the case of ICANN and contracted parties as well.

But the question is, you always need to ask whether you – whether you need all of the data that you're collecting for the purposes of the legitimate interest or whatever – or the compliance with contract or whatever the lawful basis is, the data minimization principle applies and you need to look at whether you're collecting data that you do not need for the legitimate – for the lawful bases for – for your processing.

When and where has the necessity of currently collected data informally established to date? So, I mean, I think this is a – it's an important question. Whois is a legacy system, the elements of Whois are generally the product of legacy processing. And I do think that we have had an awful lot of conversation over the past many years about what information is necessary to be collected for the various purposes and interests described.

So I was just reviewing the final report of the Experts Working Group. There are a bunch of – there's a long discussion and many charts that talk about what information might be appropriate in connection with various purposes. ICANN did go out and create the various user stories that were another articulation of the various –what data elements are necessary for whom and under what circumstances.

I think there would be, I mean, I think ultimately if you know, in an ideal world what we would have is a matrix that says here are all of the legitimate interests associated with processing personal data in the context of domain name registration and ICANN. Here are the third parties – the parties – and I'm including third parties who are entitled to invoke those legitimate interests, the circumstances under which they are entitled to invoke those legitimate interests and the safeguards that need to be in place in order to make that legitimate.

That's a major undertaking and I think you know, we have bits and pieces of it everywhere, certainly the, you know, some of it is laid out in the temp spec. But I think that, you know, the hard question here is how do we get

comfortable that those assertions, because what they are right now is essentially assertions, that those assertions – that the data protection authorities actually agree with those assertions and that the assertions have been articulated with a sufficient degree of granularity so that we actually know when you can invoke – when you can invoke that interest, who can invoke those interests and ideally we would get data protection authority sign off on that wonderful matrix.

Now I think that there are a lot of people who express grave reservations that you could actually do something sufficiently granular to get a data protection authority to sign off on those. And that's partly why we find ourselves in the situation of having a temp spec that says that registries and registrars have to provide reasonable access to those with a legitimate and proportionate interest, that's a restatement of the law. Until we move to a different state where it's clear for example, that ICANN could make decisions without exposing contracted parties to unquantifiable risk, the decision about, you know, how those legitimate interests play out in each context is left to the contracted parties.

I think ICANN has some discussion, a significant amount of discussion in the most recent document associated with the UAM about whether there are ways in which we can provide – move to providing a more predictable experience by reducing risk and therefore compensating for sort of different risk tolerances between – among contracted parties.

Which legally speaking, is likely to be the bigger risk to security and stability of the DNS enforcement by the DPAs against ICANN and contracted parties or Whois as it's currently running? I think that's – I mean, the truth is I think both of these things are significant risks. We can't quantify – because we just don't know how data protection authorities will enforce this GDPR in the context of domain names and ICANN. So we can't quantify that risk very well. Obviously ICANN – the ICANN Board does think that Whois, reasonable

access to Whois data, is an important part of ICANN's mission and is a critical feature in preserving security and stability.

The current balance here on this is to require registries and registrars to provide reasonable access to data for legitimate and proportionate and interests and at the moment in the first instance, it falls to registries and registrars to determine, to make a determination about that. If registries and registrars are not providing reasonable access in situations where ICANN believes access is warranted, then I think you know, it falls to ICANN to enforce the temp spec.

How would the data protection authorities – how would order controller processor to cease processing all data likely affect ICANN and the contracted parties? Well, I mean, it's hard to imagine that registrars and registries could actually provide the service that they do if they were not permitted to process at least some persona data, so I think that that would be a significant problem. As I said, you know, at the fundamental levels, registrars have a certain amount of information that they must process to provide the service and it seems unlikely to me that that – that's clearly a lawful basis for processing data so it's hard to imagine a situation in which a DPA would tell them to stop processing data for the lawful purpose of providing a service.

Can ICANN legally force a contracted party to disclose registrant data? So here's the crux of this. ICANN is a body that has contractual relationships with registries and registrars. It has the ability to impose obligations on registries and registrars through contracts including through consensus policies which by the terms of the contract are automatically passed through, imposed and binding on registries and registrars.

There is of course, a caveat to that which is at ICANN cannot impose obligations on registrars and registries whether those are via a specific contract provision or via consensus policy. It cannot impose obligations that require a party to the agreement to be in violation of the law. So ICANN

cannot force registries or registrars to violate GDPR and provisions in contracts that are held to violate the law are generally void as a matter of legal principle. So yes, ICANN can enforce contractual provisions including consensus policies, so long as those contractual requirements comply with applicable law.

Who decides what reasonable access to redacted Whois data actually is? Well, in the first instance under the current arrangement, that registries and – or that registrars and registries who are providing the Whois service ICANN has enforcement authority where it believes that the contracted parties are not living up to reasonable access. And surely there are, you know, there are likely to be some dispute about that in which case the enforcement, the ICANN contractual enforcement process has to wade through.

Now I know, you know, people – a lot of people are talking about ICANN wasting money on legal processes, court cases and the like, but in some cases, you know, getting sort of driving this down to the ground and getting clear information about this – unless we can get real guidance from data protection authorities, which has not been forthcoming so far, it comes down to, you know, what ICANN views as reasonable access versus what the contracted party views as reasonable access.

And it may be that, you know, that enforcement actions including resort to appropriate dispute resolution processes, court cases and the like, is what we need to get there. We're really hoping that we can get clarification through the UAM process and that obviously is much more ideal than an endless series of legal cases.

Under GDPR, is the consensus policy sufficient to memorialize the data processing agreement or joint controller agreement or would temporary agreements be required? So I think that it's hard to say – to answer this in the abstract but it seems to me that there are going to be sufficient elements that don't fit into the – so the policy permit that probably we're going to continue to

require separate data processing agreements, although they may refer out to consensus policy in the end.

As the roles and responsibilities of parties involved in processing are key to identifying and defining purposes, we feel it's important for the EPDP to identify and evaluate the parties involved in the domain lifecycle as a prerequisite to identifying purposes. Do you think it's consistent with the GDPR and good data protection practices? Yes, I certainly do think identifying the parties involved in domain lifecycles is consistent with GDPR and good data protection practices.

I think there is a lot of preexisting work on this so I'm not sure we need to reinvent the wheel. And of course I don't think that we need to think of the EPDP as the – as the process that resolves this once and for all. It would be nice if we could do that but I think that the critical issue is what can be done, what consensus can be reached within the year-long period that we have for turning a temporary spec into consensus policy. That to me is really the critical issue and there needs to be some prioritizing going on.

The consensus policy would provide baseline guidance for contracted parties based on the shared requirements of existing, however, as we conduct an analysis of the roles and responsibilities becomes clear that a data protection, a DPA, I think that means data protection addendum, or data processing agreement, a joint controller agreement or a code of conduct would be necessary to implement any consensus policy that you see in the GDPR way. Can a mandate for contracted parties and ICANN to establish these documents be an output from the EPDP? Yes, I think that that – yes, there has to be the kinds of agreements that get laid out here and I think that if that's the way the community wants to go that could be an output of the EPDP.

So, I have gone through these questions here. I keep losing connectivity. And now I cannot see the screen at all. Can you guys hear me?

Marika Konings: Yes we can.

((Crosstalk))

Kurt Pritz: Sure we can, Becky.

Becky Burr: Okay. So I can't see the screen at all; I don't know why I've lost connectivity but if you want to ask me questions while I see if I can get back into the room here I'm happy to do that.

Kurt Pritz: So Mark from Microsoft has a question and then Becky, there were some questions submitted, you know, after we sent these to you so I can ask those people that sent questions in might raise their hand. But go ahead, Mark.

Mark Svancarek: Yes, Becky. It's Mark for the record. Two related questions, right now queries for Whois data go to the contracted parties, in a couple of proposed alternate models, we could have all queries go to ICANN, for instance, in one model, queries go to ICANN and in real time they pull the data through an RDAP connection and they are the ones who reveal it to the end user. And without getting too far ahead of ourselves and getting into access issues, the idea is that at that point they could evaluate the lawfulness of the request and the appropriateness of the data requestor.

So the first question is, is there any benefit to the contracted parties if we were to take that model? The second one is related, if you've read the Eco Guidebook, you know that that there was a proposal called a Trusted Data Clearinghouse, there's a similar discussion in the Trachtenberg memo. And in that case, queries go to ICANN but ICANN is actually a co-repository of the data and so at that point there is no outreach via RDAP, the data is already in ICANN's hands. What is the benefit to the contracted parties in either of those models?

Becky Burr: So that's a really good question and I think a lot of us have been talking about looking at whether I think in one case it's referred to as kind of hub and spoke model where there's, you know, ICANN does accreditation and then although the databases remain distributed, ICANN reaches out to collect the data. The question would be would that mechanism allow us to understand and limit the risk associated – the risk to contracted parties? And if so, that would enable us to provide a much more predictable and uniform experience for users because instead of having everyone in the ecosystem making their own risk tolerance assessment, ICANN would make a risk tolerance assessment and take the- carry the risk of that.

That obviously would be something that it would have to do based on, you know, fiduciary understanding and the like. But I think if we can get some clarity that that actually would help transfer the role of data controller to ICANN, then that would be a very useful way to proceed. We don't know the answer to that and currently, you know, the view that we have heard from Article 29 is that contracted parties and ICANN are joint controllers and under GDPR joint controllers are all liable.

But I think that is a – that is a promising – that is a promising way forward and one that we certainly are interested in seeing ICANN pursue to see if we can get some clarification.

Mark Svancarek: Yes, thanks for that clarification. It was also my – it was my expectation that that structure would make the contracted parties into simple processors as opposed to co-controllers so thanks for confirming that.

Becky Burr: Well I don't – I just want to be very clear, I don't think we know for a fact that it would. It is something that I know ICANN is exploring and if it – and if it would cabin that risk it would be very beneficial. Should I just go up to the queue? We've got Marc.

Kurt Pritz: Okay go ahead.

Marc Anderson: Hi, thanks. This is Marc Anderson for the transcript. I just wanted to, you know, follow up on something that was said there, you know, you mentioned, you know, controllers and joint controllers there. And, you know, the whole conversation around, you know, controllers and processors, joint controllers, co-processors, sub processors, you know, I think a lot has been made on that and, you know, I think there are a lot of different schools of thought on who has role there. But, you know, Becky, I'd like to ask, you know, do you have a device for this, you know, this working group on how – on how we should consider each of those roles and how we can navigate that, you know, especially considering all the conflicting opinions out there and maybe some advice on how, you know, a DPA might view some of those things?

Becky Burr: I'm not sure I understand why the roles are conflicting. I feel like registries, registrars and ICANN have both individual roles and they have overlapping roles. I'm not sure conflicting makes sense to me.

Marc Anderson: Sorry, Becky, can I clarify?

Becky Burr: Yes.

Marc Anderson: Sorry, I wasn't say that they have conflicting roles, I was saying there are, you know, there are conflicting opinions on I guess what label to attach to the different parties involved. And so I've heard people lay out arguments, you know, for different parties to be assigned different labels, as far as, you know, processor, you know, controller, you know, joint controller, co-processors, you know, and I think you could probably find an argument for any number of different labels to be applied. And I'm just looking for your advice on how, you know, we as the working group can navigate, you know, those questions.

Becky Burr: Well I think that the best legal guidance that we have right now, I don't know if "best" is the right word, the clearest legal guidance we have right now is that the – is that the data protection authorities Article 29 Working Party has said

that with respect to Whois registries, registrars and ICANN are joint controllers. I suspect if you try to turn a registry into a mere processor, through a label, notwithstanding the fact that the Article 29 Working Party has said something different you're going to get resistance because the assumptions about liability will be different depending on the role when – and in the absence of, you know, a blessing from the DPAs, that's taking a significant risk.

So I think that my advice to you is to consider that under the current structure, unless we come up with something outside of this, unless we come up with something outside of this like the hub and spoke model, that – and we get some clarification that that addresses risk, I would assume that everybody in this who's providing this will view themselves as a data controller and make risk assessments based on that exposure. I think Thomas is agreeing with me, if parties jointly determine the purposes and the means of processing, that makes them joint controllers regardless of what we say.

So my view is under the current circumstances I wouldn't spend a lot of time trying to persuade registries and registrars that they're mere processors because I don't think you're going to get anywhere because I don't think there's a basis for it at this moment in this current structure.

Okay, I see…

((Crosstalk))

Becky Burr: Yes, go ahead.

Kurt Pritz: Oh this is Kurt. I know there were some written questions submitted after the deadline. Ashley Heineman, the us AC rep submitted a question so maybe I could call on her to reword, you know, rephrase the question and then go to Benedict.

Becky Burr: Great.

Ashley Heineman: Thanks, Becky. This is Ashley. And actually I posted this on behalf of Laureen Kapin who couldn't join us today from the Federal Trade Commission. She basically just points to, you know, the number of Whois policies that are being pursued by ccTLDs in Europe in particular and references the dotEU domain and where they provide, among other things, for publication of a legal person's organization name, email, city and country and a natural person's email address. And from your perspective, is this an indication that such an approach is GDPR compliant or not? Thanks.

Becky Burr: So first of all, in the case of dotEU and other ccTLDs that have either local law or regulation that apply to them, they are entitled to invoke the public interest as a lawful basis because the public interest is laid down in a relevant European or member state law or regulation. So to the extent the dotEU regulation says if somebody ticks a box that says they're a – that they're a legal person then it's okay to include personal data in the contact information. That is a luxury that ICANN doesn't currently have to rely on because ICANN, notwithstanding its global public interest role, is not recognized as a source of public interest under GDPR.

The – what we know in this respect is that the Article 29 Working Party was quite clear in its correspondence with us that one need not – that GDPR does not apply to registration data about a legal person however, it went on to say specifically – but you can't include personal information in the Whois output. So that if there was a way to ensure that if you checked a box that said, I'm a company, I'm a legal person registering this data, and you could ensure that nobody put, you know, nobody from Neustar put Becky.burr@team.neustar in as the admin contact, or the tech contact, because that would be personal information and that is what the Article 29 Working Party said must be removed from the registration – the publicly available registration data.

So I'm not sure I – I mean, I understand what EU's actual practice is or at least was because there was some rumor that they were changing things, but I know that for quite some time essentially if you said this – the registrant is a legal person then all of the contact information went in even if was personal data. I'm not ensure certain that's exactly what the – that's what the regulation on dotEU specifically says, that's how EurID has interpreted it. But I think that is absent a regulatory approval for that behavior, that's inconsistent with the guidance that we've received from the data protection authorities.

Kurt Pritz: Okay, Benedict.

Benedict Addis: Hello, Becky. Very nice to hear your voice and thanks for all your help so far. I had an idea and I'd like to run it past you in this – in front of this group which is that rather than trying to muddy the waters with lots of co-controllers, instead acknowledge that there are essentially two different data flows going on here, one of those is the contractual data flow you're familiar with of registrant gives data to the registrar and so on up the chain where it's pretty clear to me that the registrar acts as a controller and either solo or jointly with the registry.

And there's a kind of – what I've described as a quasi-regulatory flow where ICANN is making some – determining some regulatory purposes from top down and that those apply. And to me it's pretty clear that ICANN is acting as a controller in that respect, everybody in the chain is acting as the processor. Do you think there's any sort of value in separating those two flows and just defining the purposes more clearly so we're not – and the reason I got here was just thinking that otherwise we're kind of trying to put purposes in other people's mouths which gets – which is funky enough with the contracted parties but gets really painful when we're trying to imagine possible purposes for third parties which we sort of fudged so far as defining a third party interest. Thank you.

Becky Burr: Yes, so here's the problem, if that would work it would be nice. The problem is that controllers, when they release this information to a third party and that they, you know, they continue to be responsible for that third party use of the data, so if you haven't, you know, unless you can get meaningful indemnification from every party to whom you release information, you're kind of on the hook for their processing or potentially and therefore in order to sort of identify an acceptable level of risk, it's hard not to say here's what I, as a controller, deem to be legitimate interest of third parties and that's what I'm willing to be on the hook for in a certain way.

So I think, you know, it's an interesting process but I think it's very hard not to – not to take into account the fact that there's liability for onward transfers and simply saying, you know, you're going to only use it for a legitimate and proportionate interest when you're providing the information, you know, widely according to, you know, uncredentialed groups, not subject to a code of conduct, for example, would be a hard risk for folks to take.

Benedict Addis: If I may follow up? I completely agree about the risks of onward transfer and so I guess the secondary part of this proposal is that anyone seeking access to registration data in a kind of more than one off way would be expected to considered to be deemed as a controller as well. So for that just separating all of these flows out so that the contractual flow has a designated controller, the regulatory flow has a designated controller and then the access flow, so the final bit of the puzzle which you mentioned also has a controller and that's the people who want the data; they get to determine – they have to determine how the data is used for their own purposes but they're also bound by GDPR as a controller.

Becky Burr: So I think I suspect, I mean, I can tell you, for example, that Neustar does require people who are accessing this information to agree to model clauses. We view this as an onward transfer, so when we're disclosing information we impose model clauses and it is controller clauses that we use. That's an important, you know, that's an important thing that is required for – to make

our – any onward transfers legal so it's necessary but I don't think it's sufficient to cabin the risk that somebody says they're using it for a legitimate purpose and then they do something outrageous with it, it's just a risk that you know, everybody has to calculate.

Benedict Addis: Fair enough.

Kurt Pritz: I note – I know Thomas Rickert had submitted actually several questions so Thomas, could you…

Becky Burr: Oh no, hard questions.

Kurt Pritz: Yes.

Becky Burr: Be polite, Thomas.

Kurt Pritz: Go ahead, Thomas.

Thomas Rickert: As I'm always. Hi, Becky. Good morning, good afternoon and good evening, everyone. Becky, a few questions for you. So I'm not sure whether to speak on behalf of the Board, but in fact, I guess there is a risk for our group to allocate responsibilities for certain processing activities and determine who is a processor where joint controller situations are present and the like. And then, you know, to present these in our final report, get the adopted by the GNSO Council to find out that ICANN Org does not agree to such allocation of responsibilities.

So my question to you is how do we make sure that we don't run the risk of our recommendations to be rejected? Is there any possibility for the Board to engage early or for ICANN Legal to closely monitor what we're doing to make sure that we're not running into such situation?

Also, and that's sort of associated, it would be most interesting for our group to understand what ICANN is doing with personal data when it comes to compliance action, for example. So it would be very interesting for us to see a record of processing activities established by ICANN Org if one has been written so that we can better understand what ICANN is using that data for. And maybe it would be good to have a person inside ICANN to liaise with us on that.

And, you know, I have a couple more questions but just one last aspect, our charter is quite narrow with respect to what data we can actually analyze. But in fact there are more data elements that registrars are required to process based on consensus policies and the RAA. And the system, as you know, will only be compliant if all the data elements that are processed are processed in a compliant fashion. So how can make sure that the other data elements that we can't deal with are analyzed for the legality and that this is actually put into the information that needs to be passed onto registrants and the like. Thanks so much, Becky.

Becky Burr: Thank you, Thomas. So let me take the questions in order of difficulty. First of all, I am not speaking for the Board nor am I speaking for Org, I'm just trying to be a helpful party in a conversation at this moment. In terms of other data elements that are not part of the temp spec but that are required to be processed as part of the RAA, that to my mind, and I'm speaking off the top of my head, seems to me to be contractual and that the best place to deal with that is in contractual discussions between the contracted parties and ICANN Org.

And, you know, I don't know whether there have been an effort to raise those or not but, you know, you don't have to go straight into contract negotiations but it does seem to me that the contracted parties and ICANN have an interest in looking at any other data elements required to be collected and processed for compliance with GDPR.

With respect to ICANN's use of personal data in connection with compliance activities and the records of processing activities, I'm going to defer to – in particular to Dan Halloran on that, ICANN – Dan is ICANN's Data Protection Officer and so and I know I saw his name on the list of attendees so I will defer to him on that. But it's an interesting point.

With respect to the allocation of risk, I guess – and roles – I'm a little puzzled by the notion that this group is going to assign roles to folks but if you can actually get, you know, if the contracted parties who bear the risk of whatever role is assigned to them and they're the risk of this group getting that wrong, since, you know, if you're a controller you're a controller no matter what you call yourself, then I think you know, with – it's an interesting activity assuming that it can be done in the time allotted.

There are two Board liaisons – Leon Sanchez and Chris Disspain, who are closely following the work of the EPDP. And I know that they are paying attention to these kinds of things. The Board is taking – is very interested in us, we are getting briefings and updates from Leon and Chris all the time and our goal is of course not to come in under any circumstances at the last minute and say wait, wait what you've done is wrong. We will certainly, if an issue comes up that causes concern, that would certainly be something that we come up with.

But I'm just curious and I know we have only a little bit of time, but I guess my question is under the current circumstances, so what – where we don't have, you know, some hub and spoke model or some other alternate that might help us say with affect and meaning that, you know, contracted parties are processors as opposed to controllers, what the point of assigning the roles is. And maybe we can take that off…

((Crosstalk))

Thomas Rickert: Becky, if I may?

Becky Burr: …and I'm just misunderstanding…

Thomas Rickert: Let me try to clarify if I may, Kurt? We might establish that ICANN, the registries and registrars, are joint controllers for certain processing activities. That requires these parties to enter into a joint controller agreement. The same will apply to escrow and EBERO where we might determine that ICANN is the controller and the escrow agents and the emergency backend operators are processors. Those require written agreements between those parties. So if we make a recommendation to that effect and find out that ICANN actually refuses to enter into such agreements with those parties, then I think we would have exactly the situation that I'm afraid of and that I'd like to avoid.

Becky Burr: Okay. Okay, well I think that – I think it's very important then for – that ICANN Legal, including Dan and the Board liaisons should be closely monitoring the work and raise a hand in the event that they see something uncomfortable coming down the line to resolve those issues early. As I said, the Board, not just in this context but in all contexts, has been really trying hard to get out in front of these issues early on. The last thing we want to do is essentially, you know, have people going down various alleys and tunnel that are not going to result in workable outcomes.

Kurt Pritz: Hi, Becky, this is Kurt. I'm sorry, I didn't know if you can see the screen yet or not. Diane Plaut of the IPC has a question.

Becky Burr: Go ahead, Diane.

Diane Plaut: Thank you, Kurt. Just to follow up on what – thank you. Hi, Becky. Just to follow up on Thomas's points, it's clear in our EPDP to date that it's very much an evaluation of time to assign roles to make all the different states comfortable and certain about risk allocation. And that's very much a key issue, which is understandable. That's why it's very important for – to make

any type of temporary spec and consensus policy work to understand how ICANN is going to address that risk.

And in doing so, to also understand is there going to be an underlying Article 30 record of processing, technical and procedural safeguards document, retention policy, data subject access rights policy, etcetera that ICANN is going to make available as a joint controller particularly in the case of a unifying access model so that the risk allocation is not only accepted by ICANN but that the if contracted parties as well as IP owners and all the other stakeholders involved could be clear on ICANN's ability to provide a GDPR-compliant and data practicing compliant background and basis going forward for the processing of personal data? So any input by ICANN and to ICANN I think would be very essential to us in moving our agenda forward.

Becky Burr: So I'm going to defer to ICANN Org on the specifics on your question but let me just answer that by saying, I think Göran has been very clear both publicly and in conversations with all of us that the key to, you know, one approach to providing a more predictable experience is to effectively cabin risk and have a central risk tolerance decision made by ICANN in the hopes of clarifying sort of controller liability, in any particular case, and I would assume that anybody who views themselves as a controller, which one would have to do in order to have a sort of centralized clarification about liability here, would be well advised to comply with all of the documentation requirements in GDPR including records of processing activities and the like.

Kurt Pritz: All right then, so that's a pretty timely close. Unless somebody has a final comment? Gosh, Becky, this was great. It was content-packed and interesting and I've made a commitment to myself to go back and listen to it again to make sure I caught everything. So on behalf of all of us…

Becky Burr: Oh no. If I said anything wrong, it was a mistake.

Kurt Pritz: When I say something right it's a mistake so you're in better shape than me. So thanks very much for taking the time with us and you know, I'm going to just mention that since you've been so generous from time to time if we have questions we might send them your way but thanks again and everybody have great day and we'll talk on the call tomorrow.

Becky Burr: Great. Thanks, everybody.

Terri Agnew: Thank you, everyone. And once again the meeting has been adjourned. Operator, if you could please stop all recordings? To everyone else, please remember to disconnect all remaining lines and have a wonderful rest of your day.

END