ANDREA GLADON: Good morning, good afternoon, and good evening to everyone. Welcome to the first webinar of the 2018 AFRALO hot topics [webinar] on the topic of compliance of the WHOIS registrant data with the GDPR on Thursday, the 23rd of August, 2018 at 18:30 UTC. Our presenters today are Thomas Rickert and Stephanie Perrin. We will not be doing a roll call, this is a webinar.

We have French interpretation, so please, I remind you to state your name before speaking to allow our interpreters to identify you on the other language channel, and for transcription purposes. Please also speak at a reasonable speed to allow for accurate interpretation. Could I kindly remind all participants on the phone bridge as well as the Adobe Connect to please mute your speakers and microphones when not speaking? Thank you all for joining, I will now turn it over to Tijani Ben Jemaa, the chair of the At-Large capacity building working group. Over to you, Tijani.

TIJANI BEN JEMAA: Thank you very much, Andrea. There is someone whose microphone is very noisy, so if there is a possibility to mute him, it'd be very good. Okay. So good morning, Stephanie. Good afternoon, good evening for all the others. This is a specific webinar for AFRALO hot topics working group. They asked for it, they identified one of the hot topics for AFRALO is the compliance with GDPR of the registrant data, and they asked for this webinar. That's why we are organizing it today for them. So it is specific for AFRALO and not for the whole At-Large community. I

want to remind you that there is French interpretation, so people who don't speak English can follow the webinar.

Our speakers today are Thomas Rickert. We had it before, we had a webinar about the same subject before, and Thomas came and presented, and I would like to present him again because he's always helpful and is always available. Thank you very much, Thomas. The second speaker today is Stephanie Perrin. Stephanie is one of our friends, she is from the NCUC, and she's one of the most passionate persons about data protection. So I think she's really the right person for this webinar. Before we go to the presentations, I would like to go back to the staff for some housekeeping items. Andrea?

ANDREA GLADON: Thank you, Tijani. I'll run you through a few housekeeping items before we start. For questions and answers during this webinar, you can submit these via the chat pod by typing the word "question" followed by the actual question. These will be directed to the presenters. Please do however note that we have a question and answer session after the presentation and pop quiz questions.

Regarding the pop quiz questions, we'll display these after the presentation, so for all of those again in the AC room, please be ready to answer the questions via the polling tool on the right-hand side of your screen. Thank you so much, Tijani, and back over to you.

TIJANI BEN JEMAA: Thank you, Andrea, and now I would like to give the floor to Thomas Rickert who will start the presentation Thomas, please.

THOMAS RICKERT: Thank you very much, Tijani, and good morning, good afternoon, good evening to everyone. Tijani, thank you so much for your kind words, and it's always a pleasure to be with you. And since I've only spoken at one of your earlier webinars, I will not go through the legal basics of GDPR. I think we've done that already, so I think, should you have any questions with respect to the legal aspects of what I'm discussing, please let me and the rest of the group know via the chat pod, and I will answer your questions as good as I can.

What we've done in preparation of this call is [inaudible] a little bit what we're going to discuss between myself and Stephanie Perrin. Stephanie is a real expert on all this. So what I'm going to go through is where we are at the moment, the implications of the temporary specification, the expedited policy development process that has started earlier this month, and some of the issues that are not yet resolved but that are subject to debate inside this EPDP group and on which I hope we can converge to consensus in the next couple of months.

Also, I will share with you my take on some of the questions that are unresolved at the moment, so you can form your views and either agree or disagree with my suggestions. Before we dive into the agenda, let me also briefly say an addition to what you'll find in my CV, which I think has been linked to in the invitation on the website. I'm a lawyer by profession, I am managing partner [inaudible] specializing in IT-related

matters. I personally have been working in the domain industry for almost 20 years now, and one of the areas in which I consult is data protection.

And in that regard – and that I'm just mentioning for full transparency – my firm together with another law firm, Fieldfisher, our firms are currently representing a registrar based in Germany called EPAG, defending this registrar against a filing for preliminary injunction that has been issued by ICANN. Exactly the scope of what ICANN can request registrants to do under the new regime, under the temporary specification. So I think that's something that you should know.

And also, I guess you see this from the design of the slides that I'm using, I'm working with ECO, an Internet industry association based in Germany which has more than 1000 members in more than 60 countries around the world, so it's quite an international organization, and I'm responsible at ECO for everything related to DNS and the domain industry. So I'm trying to navigate our members through the challenges that occur in the domain industry, we're trying to take good care of their interests.

And one of the things that we did that you may or may not know is that when ICANN did not yet come up with its own proposal on how registries and registrars should deal with GDPR, we thought that we should be of good service to our membership and come up with a data model. And that result is in a document which we call the ECO GDPR domain industry playbook, and that is a 70- or 80-page long analysis of the data flow in the domain name industry, and we have held public consultations on this paper and produced various versions of this

document. And that document can be downloaded on ECO's website. It's also linked to on ICANN's website as one of the community models that has been submitted earlier this year.

So we've put a lot of thought into how the GDPR challenges can be resolved in the ICANN environment, and some of the thoughts that we've developed there have also gone into the suggestions that I'm going to share with you during today's webinar.

Now, what happened so far? You do know that registries and that GDPR – just go back to the proper slide – is enforced as of May 25th, and that ICANN has issued a so-called temporary specification on May 17. And I think the dates being so close, that's not a coincident, but ICANN deliberately tried to get something out there to the ICANN community and the registries and registrars in particular to give them guidance on how they should operate in a post-GDPR world. Basically, that is the model that they have suggested for registries and registrars to follow as of May 25th.

Now, you might say May 25th is too close, the temporary specification has only been adopted on May 17, and you are right. So it has been a challenge and there is a challenge for registries and registrars to comply with these specifications, but there are implementation timelines in this document as well, during which the registries and registrars have to adopt [inaudible].

I will touch upon some of the I guess more important points of the temporary specification as we go through the details of what the EPDP working group is doing at the moment. But let's pause for a moment

and think about what the temporary specification actually does. You might know that typically, ICANN working in this multi-stakeholder model, working in a very democratic way, is being very inclusive at the global level w this bottom-up policy development process. It only adopts such policies that have been developed by the community.

When it comes to PDPs for generic TLDs, that would be a PDP inside the Generic Name Supporting Organization, that has to follow a certain procedure during its development, and the GNSO council votes on it, then the ICANN board adopts it. And then once the ICANN board adopts it, it becomes binding for all registries and registrants without the need of amending the contracts that ICANN has with registries and registrars. That is the beauty of consensus policies, because they become effective without a need of changing contracts for all these individual players.

Now, in this particular case, there was not sufficient time for the ICANN community to come up with a policy recommendation, and therefore the ICANN board step in, which it can under its bylaws, so it can actually adopt a temporary policy or a temporary specification if immediate action needs to be taken to maintain the stability or security of registrar services, registry services or the DNS or the Internet.

I've quoted the section two of an appendix or a specification to the registrar accreditation agreement in the version of 2013 for you. So that’s basically a possibility for the board to pursue, and in this case, the ICANN board has done so. And that means the ICANN board could come up with a policy that is binding upon registries and registrants while bypassing the full-blown community process.

Now, can such policies last forever? No. Another quote that I've put on the slide for your reading pleasure is .212 of the same specification that we just discussed a moment ago, and that basically says that the temporary specification is valid for 90 days. It can be renewed for another 90 days and another 90 days, but for a maximum of one year.

And if during this period of time, the ICANN community has not come up with policy recommendations that can form a consensus policy to replace or confirm the temporary specification as a consensus policy, then we have nothing. Because as you can see, the registrar – this is just because I chose to quote from the registrar accreditation agreement – shall no longer be required to comply with or implement such temporary specification or temporary policy.

And this is why at the moment there is an awful lot of pressure on the community to get something done in time to replace the temporary specification, because otherwise, the industry would be in a vacuum. And this is why the GNSO council has started the initiation of a policy development process. The expedited PDP has started on August the 1st. the goal is to have policy recommendations done, or in other words for the EPDP working group to have its work completed by the anniversary of the temporary specification.

And that does not only include the work of the PDP working group but also the adoption of the recommendations by the GNSO council and the adoption of or the approval of these recommendations by the ICANN board. And therefore, the time available is actually much shorter than this one-year period. So pressure is on, and just so you know, Stephanie Perrin and myself, we happen to be members of this expedited PDP. We

already had the pleasure of having an almost two-hour call earlier today, so everyone had to commit to spending a lot of time on this. We have two calls per week, and we always g et some homework from our dear chair, Kurt Pritz in order to get the job done in time.

Now, I think if you're interested in the challenges for the EPDP working group, you should look at the charter, because the charter has all the questions in it that the EPDP working group has to resolve. And those are questions in respective areas, and we will touch upon some of those in just a moment.

Some of you will surely be interested in how information that is currently not publicized via a public WHOIS service will be made available to previous WHOIS customers, be it trademark owners or law enforcement, but during my talk, I will not discuss the question of access, that’s something that Stephanie will do during her part of the presentation.

The first deliverable of the EPDP group is the so-called triage report. And that’s basically a document to establish the level of consensus on the various aspects of the temporary specification, or actually to determine where there's divergence among the members of the EPDP working group or where there’s probably total objection by all participants against the aspect of the temporary specification.

So we were presented four questionnaires that we have to respond, each of the questionnaires covering a part of the temporary specifications. We were asked with respect to every aspect of the temporary specification, is this something that you support, is this

something that you don’t have a strong opinion on, or is this something you object against?

And it’s quite interesting, because we got overview sheets, which I'm sure will be publicized once the triage report is ready for publication. Some groups have marked most of the aspects green while other groups marked most of the aspects red. So we can expect some vivid debate about almost every aspect of the temporary specification.

And just so you know, I'm amongst those – I'm representing the ISPCP on this group. I'm one of those and the ISPs are with me. We think that there is quite substantial need for revision and additional work with respect to the temporary specification, which we think is not a document that you can make work with only minor revisions. But we have an awful lot of different views in the group, as you can imagine, because the GAC has different views than the BC, the BC has different views than NCSG and others. so as much variety as we have in the ICANN community, as much variety we have on this team. So the triage report will be report will be ready soon. The members of the EPDP group have until tomorrow to comment on the draft document, and I'm sure that it will be publicized to the wider community in the next few days.

So, let’s go through some of the issues with the temporary specification. And I should note that although we had our seventh call earlier today, we have not really – or we've just discussed substance a little bit today. The past couple of calls dealt with procedural aspects, the first couple of calls dealt with establishing the level of consensus or objection with the appropriate presentation of the level of consensus or divergence

[inaudible] in the triage report, so we've just established the status quo of where this group stands at the moment.

So I do not have any results or even interim results of where this group is at the moment, but what I will highlight for you in the next couple of minutes is on what the topics that have crystalized as being most contentious are.

Now, as you can imagine, for some in this group, the temporary specification goes too far. For some, it doesn't go far enough. [inaudible] the broad range of views. And for some, we're in a global environment, it is too EU, too GDPR-centric, and therefore, they are looking for a way to make it more generic so it is applicable more to our jurisdictions that we have around the world.

And I think this places the first big challenge on the group, because you can't really be generic in a world where we are at the moment basically responding to the back and forth between ICANN and the European Data Protection Board, previously called the Article 29 Group, and their issues that they had with ICANN's approach to personal data and potential threat of sanctions by those authorities.

So my take on this is that GDPR is amongst the strictest laws when it comes to data protection at the global level, so it's quite a high bar, and I think that if we pass the tests of GDPR, chances are good that ICANN and its contracted parties are compliant with almost every data protection law around the world. And this is not to be exclusive or not to be globally inclusive, but this is just, I think, a straightforward method

of trying to get ICANN's data protection to the next level and compliant with most jurisdictions around the world.

So let's go through some of the issues that we have identified already. So just as a reminder, at the moment, we are, in many discussions that I'm either participating in or following, everything is centering around access to WHOIS data. And if you look at this visualization, this is just a gentle reminder that we have many more [inaudible] in the world of generic domain names.

So we have Internet users that go to a registrar or a reseller there, and the registrars are accredited with registries, and both registries and registrars have different types of escrow agents where that data is [backuped.] Then, in case of an emergency, there is the EBERO, the emergency backend operator that steps in in case of registry failure. And these EBEROs, we have a couple of them around the world that have been hired by ICANN, they can also get access to all of the data that a registry has for keeping up the registrations of their registrants, of their customers.

And then we have WHOIS customers that want to get access to the data, both with registries and registrars, and then we have ICANN that requires its contracted parties to report, including personally identifiable data, at least until the pre-May 25th era, and we have ICANN that wants to get access to data for compliance action. Right? So ICANN is governing, part of this industry by issuing contracts, by enforcing contracts, we have the ICANN community that – including registries and registrars who have their respective stakeholder groups also is instrumental in crafting policies.

So a lot of players have something to say in this industry, and GPDR is a legal instrument that requires those who want to be complaint with it to take a holistic view at the data processing. And that means that you have to take a look at all steps from the collection of data through altering it, through transferring it to third parties, to disclosing it to the public possibly, to deletion. All these modifications, alterations, disclosures, deletions, processing activities, for all of which we need a legal basis and a lawful purpose.

So in order to do a good job with GDPR compliance, we need to make sure that we're looking at all those aspects. And one of the criticism that I have for the temporary specification is that it does not include all aspects of what's happening with the data. Although it's far better than other documents that we've seen earlier in the last couple of months of debate.

So these are the topics that I'd really like to go through you. Briefly, those are also [inaudible] in the charter for the EPDP working group. So purposes for processing. As I mentioned, for every processing activity, we need a lawful purpose, and there is a challenge with the temporary specification because it lists all sorts of purposes for ICANN and its contracted parties processing personally identifiable data, but some of these purposes are ICANN's own purposes, other purposes are third-party purposes such as law enforcement, consumer protection, trademark infringement and others.

While ICANN's core mission, if you wish, has more to do with ensuring that there is a stable, secure and resilient DNS, including domain names. Right? So there are discussions starting already on how to separate

ICANN's own purposes from those of third parties and how to determine whether certain purposes are within ICANN's mission and which of those purposes listed in the temporary specification are potentially outside ICANN's mission. So I think I should leave it there, because that's something that Stephanie will also say a few words to.

Then data collection. The EPDP working group is specifically tasked with looking at the question of what data elements must be collected for the registrants, for the admin-C, for the tech-C and for the billing-C. You know that before the temporary specification entered into force, before the GDPR actually kicked in, you needed to have the name, address, phone number, fax number if you have one, and e-mail address for all those contact points, and all those contact points would be published.

And that is the primary source of issues that ICANN has with the authorities so far, because they said that this unlimited publication of personal data is not appropriate, it's unlawful. And it will be the challenge for our group to determine which of those data elements shall be required to be collected mandatorily and enforceable to ICANN's compliance team.

And I'm not only discussing are we collecting registrar – registrant data, [inaudible] for a tech-C, potentially, for a billing-C, potentially, but we'll also need to take a look at whether the data elements themselves for each of those contact points are actually lawfully collected. You know, do we need a fax number these days? I don't know who uses a fax number, but some of these data elements might not be required.

So this is something that needs discussion, and as I mentioned at the outset of this call, there's currently a court case going on. ICANN has filed for a preliminary injunction with a court in Bonn, Germany, and according to ICANN's own statement, they tried to get clarification form the court whether EPAG, the registrar, can be obligated to collect the data for the admin-C and the tech-C.

This has gone on for a couple of months now, there have been a few decisions, some procedural in nature, but current status in this preliminary injunction case is that the court has rejected the application for a preliminary injunction. So basically, they said that ICANN has not sufficiently explained why it is necessary to have the data for the admin-C and the tech-C, and they particularly refer to the fact that registrants can insert the same data for the admin-C and the tech-C as for the registrant itself. So they said that there is likely not additional intelligence that can be drawn from that since ICANN does not have different requirements for these different contact points.

I'm keeping this very superficial. I have put the link to ICANN's website on the slide where you can find all the documents pertaining to the litigation. So if you want to read all that, please go there. Next point is the transfer of data from registrars to the registry. This is something that many of us sort of take for granted because they said if the registrar can have the data, then why should the registrar not be able to get the data?

As I mentioned earlier, we need to have a lawful purpose and a legal basis for that data transfer as well as for each and every other processing activity. So our group will need to sit down and discuss what

the rationale for the transfer of data for a registrar to the registry actually is. And some of you who think that this is required, just imagine, VeriSign, operating .com, does not know who the registrants are. Right? So since they're operating thin WHOIS, they do not know who the customers are, and still, this zone, which is the biggest zone of all, works perfectly fine. Right?

So one might say – I don't know what [inaudible]. The slides are flicking back and forth. I'm not doing that. I'm trying to get it back to the correct slide, and I don't know why it's moving. So we were here.

ANDREA GLADON: Apologies, I'm not sure who is moving [inaudible]. What slide were you on?

THOMAS RICKERT: 13. So I'm on 13 now, so that is fine. So basically, the VeriSign example shows that you can perform the contract vis a vis the registrant without the need for all the data to be transferred to the registries. So according to article 6(1)(b) which is performance of the contract, you might not need that processing activity.

Yet a lot of registries have a vital interest in knowing who the registrants are, because they might have an interest in examining the zone files to identify patterns of illegal behavior, perpetrators using domain names for certain schemes of abusive behavior, and they might need that data to do that. They might need it for security purposes. And that is perfectly okay, just a different legal basis, and that would be 6(1)(f) in

this case, where the registry can assert to have a legitimate interest in that data, and that could be a basis for the data transfer.

So I'm not saying it's not possible, but our group will need to work on that and come up with ideas for what's mandatory, what's potentially optional for the registrars to transfer to the registries. Then the transfer of data to escrow agents. This is something that I guess most will agree is a good idea in order to secure the data. Yet most of the registries and registrars would do t heir own data backups already, so they are required by ICANN to use certain types of escrow agents, so ICANN has a huge interest in performing its function to make the system resilient. ICANN has an interest in this data to be escrowed and to be able to take the data out of escrow to a [inaudible] registrar or to the EBERO.

And therefore, in this case – and this is something that hasn't yet been spelled out legally – there needs to be a data processing agreement between ICANN and the escrow agent and not between the escrow agent and the contracted parties as the temporary specification requires at the moment. So certainly, this will be subject to further debate, but in order to make the whole system work in a compliant fashion, we need to rethink the legal concept of the escrow agent and sort out the legal relationship between ICANN and the escrow agents for registries and registrars. And in this contractual relationship, the registries and registrars don't even have a role to play.

A [comparing] situation is present with the EBERO where the EBERO doesn't even get the data from registries or registrars, they get the data from the escrow agents based on a direction or an order from ICANN.

So one of the questions is whether this is actually a subject for the EPDP since contracted parties don't have a role to play in this.

In my view, I think these questions should be resolved in one place, and so I think it would be appropriate, as time permits, for our group to also come up with requirements to govern the legal relationship between the EBERO and ICANN in order to make sure that there are no inconsistencies or gaps in all the documentation that is required. Let's not forget GDPR is a lot about accountability, a lot about documentation and a lot about having the evidence in place that you have done your job properly in documenting all of the processing activities and the legal basis [inaudible].

Now, in my view, ICANN is the controller for this and the EBERO is the processor, and that is something that hasn't yet been put into the contract with the EBERO to my knowledge and is something that needs to be fixed in order to achieve compliance.

Then, publication of data. I'm not talking about the whole question of granting accreditations to certain WHOIS customer groups so they can [cert themselves] potentially, but I'm talking about what currently is publicized and whether what is currently publicized is okay or not. As I mentioned a few minutes ago, before the temporary specification kicked in, all data elements for the admin-C, tech-C, billing-C and the registrant were publicized, and such publication did not require to perform the contract.

You don't need to publish information in order to allow for a domain name to be registered, to function properly or to be renewed or

transferred. So we cat just take the contract with the registrant as a legal basis for publication. You would need the consent, for example, for that publication. And at the moment, there are no technical measures available in an industry-wide fashion that allow for a legally compliant transfer of the [content as well,] because each step of the lifecycle of the data element, all the parties involved would need to have proper documentation of the customer's consent or the withdrawal thereof.

So we're technically unable to have that at the moment. There's work underway, but that's not possible at the moment. And then there's a big question about is what is being redacted at the moment going too far or not. In the eyes of the BC, the GAC and the IPC if I remember correctly, they think you're redacting too much information, you could publicize more information.

At the moment, the registrant name is not publicized, the registrant address is not publicized, only the province and the country of the registrant are being publicized, and e-mail addresses, fax numbers, phone numbers are redacted. Only anonymized e-mail addresses or webforms have to be provided by the registrant. And the organization field needs to be publicized.

And that's one of the areas that I have an issue with, because the organization field – and I think suffice to say more than 60% of all domain registrations, the information in the organization field is identical to the information in the registrant field. So if you say that you can't, for reasons of GDPR, publicize the registrant field, then as a logical consequence, you can't publish the organization field. Right? So I would, from a legal perspective, even ask for more restrictive handling of

registrant data, but others say you should make a distinction based on what the customer says. If the customer says I'm a company, then their data doesn't deserve any protection. Right? And they want to do it that way.

I think that treating data as nonpersonal data based on the self-identification of a customer or a registrant is dangerous in terms of compliance, but I think it 's worthwhile reaching out to the authorities and asking t hem for advice whether they think that self-identification is good enough a measure for registrars to engage in order to be protected. And maybe they say, well, somebody who's in business, somebody who says they are a legal entity, they forebear their rights to their protection, therefore you are okay, and if there is the occasional case where this goes wrong, then we're not going to sanction you. That's a possibility, but we don't know how this is going to play out.

Then we have data retention. Data retention is [an order] by the temporary specification, so there has been the request for keeping the data for two years after expiry of the domain name, and that has not changed. The issue is that so far, we don't have a robust rationale as to why it has to be two years. And – I'm not sure, probably Stephanie will speak to the exchange between ICANN and the authorities on that point, but I think we don't have anything in the law that says it has to be two years. And in the absence of a prescriptive law, we need to come up with our own idea. Why is it not six months? Why is it not five years? Why is it exactly two years? So we need at least a point to – we need at least to come up with a rationale. And I think that probably a rationale could be in the TRDP, the transfer dispute resolution policy, and that

would be one year. Just food for thought. Others think that other time frames are appropriate.

[More issues] – and I'm going to be done with this in a moment – is that we need to talk about responsibilities of ICANN when it comes to registration data in the registration process. So in my view, registries, registrars and ICANN are deemed to be joint controllers, and in order for that to be complaint, we need to come up with a written joint controller agreement with one public part and one part that doesn't have to be publicized.

We need to discuss more how transfers can be done or whether the system for transfers as in the temporary specification is sustainable. At the moment, no data from the registrant is passed on from the losing to the gaining registrar, but the registrant has to reenter the data for the registration. We need to tweak URS and UDPR a little bit, although I don't see issues there. I think the temporary specification is fine in that regard.

We need to discuss [inaudible] access as well, because in my view, domain names can be personally identifiable data as well, and [inaudible] access is not required to perform the contract. So we need to find good reasons for keeping up the [inaudible] program that ICANN has. And ICANN's reporting and compliance, does ICANN actually need to get all the data they're currently requesting for a compliance action, or would it be sufficient for them to do that upon request?

And ultimately, or finally, the temporary specification has a lot of information in it about how registrants need to be informed, and much

of that language is actually flawed, because before we have answered the trust questions on who does what, what the roles and responsibilities are, we can't write up what information needs to be provided to the registrant. So I will conclude with this. We started substantially late, so I hope I haven't taken up more than – or substantially more than – the 30 minutes allocated to me. Thanks so much for your interest and listening to me. And over to Stephanie. Or maybe to Tijani first. Thank you.

TIJANI BEN JEMAA: Thank you very much, Thomas. You used more than it was allocated for you, but it is not a problem. I hope we will be able to have some more minutes with the interpreters. Thomas, I didn't know that your company is defending the German registrar within the litigation with ICANN, so it is interesting to know that. Thank you very much for telling us. Now, we will go to Stephanie. Stephanie Perrin, please, you have the floor.

ANDREA GLADON: Stephanie, please check your mute button.

TIJANI BEN JEMAA: Stephanie, I don’t hear you.

ANDREA GLADON: Stephanie, your line is not muted on the bridge, so you should be able to speak on the audio bridge. Perhaps you muted your phone.

TIJANI BEN JEMAA: To unmute, Stephanie, star seven.

ANDREA GLADON: Just one moment. I'm going to have the operator try to pull her out to see if she can get a response.

TIJANI BEN JEMAA: It seems that because Fatimata is able to hear Stephanie, but I am not able to hear her.

ANDREA GLADON: Okay. Give me just a moment. I wonder if she was speaking on the AC and it wasn't –

TIJANI BEN JEMAA: French channel.

ANDREA GLADON: Yeah. She was speaking on the audio bridge, I couldn't hear her. Okay, just a moment. Stephanie, the operator tried to pull your line out of the audio bridge, and she wasn't able to get an answer from you. I'm not sure if maybe you're speaking on the AC line and we're having some issues for the people on the bridge. Because I'm on the bridge and I cannot hear you. Yes, it sounds like that people that are on the AC line

can hear you, but the people on the bridge cannot hear you. So if you could speak on your phone into the phone bridge.

STEPHANIE PERRIN: Okay. How's this?

ANDREA GLADON: Yes. Thank you, Stephanie.

STEPHANIE PERRIN: Okay, very good. I hope everybody can hear me now. Just by way of introduction, I have been participating at ICANN for the past five years. I was more or less recruited to join the expert working group that worked on the WHOIS issue back in 2013, and I must say, that has lured me into participating at ICANN because of what I regard as remarkable intransigence in not accepting the reality of data protection law.

I have worked most of my career in the Canadian government as a data protection officer, data protection director in many government departments, someone who worked on the legislation that passed in 2000 and for the private sector, and then later in the office of the privacy commissioner as their director of research and policy. So I've kind of done data protection from a multitude of angles. That doesn't mean anybody's listened to me since I've been at ICANN, but I hope I can bring some insights into how people look at this from a data protection perspective if you're working in this business. Now, let me see if I can get the slides to move for us.

Okay, so briefly, I wanted to go over just a quick history of the WHOIS struggle at ICANN, some of the factors important to the determination of purpose, a brief discussion on the access to data versus inclusion as a purpose of processing. This is a problem that we have been struggling with in the last probably three RDS WHOIS working groups.

And then I want to talk to you a little bit about standards for disclosure to third parties, because it doesn't seem to be something that people understand well here. And then we can talk about the quiz and questions. And I'll try and make up some of the time. According to my clock here, it's 3:30 in the afternoon, and we end at 4:00. So we'll have to move very quickly to allow time for questions.

So basically, there has been discussion lately in the experts – in the EPDP working group that has been established to deal with the temporary specification about the whole purpose, the importance of defining what the purpose of processing is. And I describe it as the purpose of collection, use and disclosure, because these are often different purposes.

A broad interpretation of the purpose of the collection, use and disclosure, in other words if you were to define that as basically anything related to the DNS, well, then that indeed would allow you to disclose personal information that is gathered for the purposes of registering a domain name for all kinds of other reasons.

ICANN's remit is very narrow, so data protection experts are fighting this broad interpretation. Purpose limitation is the first premise of data

protection analysis. The purpose must be narrow, proportionate, tightly related to the mission of the organization, not broad and vague.

I would also say that controllership is an issue that ICANN has not yet addressed. It's vague in the temporary spec, and determining who's the controller is important in terms of the GDPR, so this is something that we need to address rather quickly. Now, here is – and I apologize for the different colors on the screen, I'm afraid it didn't show as different colors in my system, so whatever I've done, I apologize. I'm sure you'll live with it.

I would argue that the policy that currently prevails, or did until the temp spec came, was set out more in the registrars accreditation agreement than in any other document that ICANN has prepared. The WHOIS data delivery requirements are stipulated here, precisely what has to be collected and what has to be put into the directory. The registrant data collection and retention requirements for law enforcement purposes are in here, and the registrant data that needs to be escrowed is in here.

Now, the third bullet here says registrant data escrowed in the U.S. for recovery and legal issues. This is an important point that came into focus back in 2014 when the safe harbor mechanism was thrown out by the European Court of Justice because it did not meet the adequacy standards that were demanded by the previous data protection law that applied, laws that basically had to conform to the 95/46 directive.

So the court found that the Article 29 working party had erred in recommending that the safe harbor initiative be accepted and that the

commission had erred in accepting it, in the European parliament, of course. So that immediately raised the question then, was it safe to send European data to the U.S. for escrow purposes? Just noting that here in passing.

The data has to be available for bulk processing by third-party service providers, that's right in the RAA agreement. And that runs completely counter to requirements in data protection law. You don't provide personal data for bulk processing. So these are just examples of things that in fact have long violated data protection laws.

Now, here is some of the factors and the analysis of this situation. ICANN is the data controller in my view, ICANN sets the terms for policy through the GNSO policy development process, and at the moment, in the absence of a comprehensive WHOIS policy, that policy is set by the contract to which it is a party that controls the compliance of the registries and registrars. So that, in my view, makes it the data controller.

Registrars in my view are data processors with respect to all data mandated by the RAA, and they're controllers for the customer relations data. Many of the organizations that actually manage domain names are resellers of all kinds. They have customer relations, they may provide hosting. The individual that is employing them may have no real idea how this all works at ICANN, [no more] should they. The registries are data processors with respect to the data required by their contracts, including PICs, public interest commitments.

So the purpose needs to be established in the context of ICANN's mandate and mission, which is a narrow one. And that narrow mission has just been re-ratified in the recent IANA transition and the new bylaws. There are certain things relating to WHOIS that have been grandfathered, but this all needs to be reevaluated in the context of data protection law and the GDPR.

So what have the EU DPAs said? I have thrown in a couple of slides here because there is a prevailing rhetoric going around that this is new and it snuck up on us and that GDPR couldn't have been anticipated. Well, I don't doubt that ICANN slept through the passage of the GDPR, and the two years that we could have spent getting ready for it were unfortunately rather wasted arguing in the RDS PDP that has just been put on hold for the moment, but in fact, the EU data protection authorities have been very active in pointing out, in writing to ICANN, in issuing opinions for quite some time.

So I'm just going to skip through these slides, you can look at them later. Basically, they've been at it since 2000, and most recently in 2014, Peter Hustinx, who was at that point the European data protection supervisor, now replaced by Giovanni Buttarelli who came to visit ICANN in Copenhagen last year, he basically wrote to ICANN informing them that their data retention practices required by the RAA were no longer complaint with the EU charter of rights.

So there's been no lack of input on the data protection side at the side of the commissioners. In terms of this whole problem with purpose, there is a very important opinion that was published by the Article 29 working party in 2013, and I think it's worth a read, frankly, if you're

trying to understand what the data protection authorities are looking for in terms of purpose. Yes, it's 2013, that predates the actual passage of the regulation, but it is the way the data protection authorities who are still around – it's not the Article 29 working party anymore, it's now the European Data Protection Board, but this is how they think about purpose.

And my next slide, I have pulled out the key things from the executive summary there. In particular, account should be taken of the following key factors. The relationship between the purposes for which the data has been collected and the purposes of further processing, the context in which they've been collected and the reasonable expectations of the data subjects. That's pretty important because it's very little outreach to data subjects about their rights in the history of ICANN.

The nature of the personal data and the impact of the further processing on the data subjects, and certainly at the Noncommercial Stakeholder Group, we argued strenuously that publishing address and phone number and e-mail exposes registrants to all kinds of harm these days. And that's fairly well understood. It doesn't seem to be acknowledged in the ICANN context.

And the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects. That's also critical because this data is being gathered by third parties, value added service providers, and used for all kinds of other purposes that may impact on the registrant's right.

So here are some ideas of how we could solve this. Have the purpose match the narrow ICANN remit. Have a look at the actual rationale for public safety actors and private sector security firms to get easy access to the data. The data commissioners in particular have written to us specifically and said it is not ICANN's role to set up a data repository for simplified access to personal data for law enforcement. I mean this is a fight that the data commissioners have been fighting in just about every country with respect to telecom data, ISP data. It is very similar data, dan the fact that ICANN was set up to provide a free repository in the face of numerous legal battles going on in different countries, I would say undermines the good faith proposition that law enforcement needs access to this.

There is a risk of the RDS data collection purpose being broadened through the public interest commitments. I don't think we have time to go into that deeply, but that whole public interest commitment thing in the new top-level domains can just be seen to justify us getting into content regulation. And I just note in passing that there are language barriers in these discussions. I have often, as we sat through the RDS working group over the past two years – and I expect to do it again on the new one, the EPDP – people translate these terms differently. In the data protection world, we don't talk about use cases. In the engineering world, we talk about use case. That's happening at a field of endeavor level, but then there's the whole problem with translation services and how these expressions are being translated. I think it's problematic, particularly when we've never defined the terms.

So access to data versus inclusion as a purpose of processing. One of the principal fights that's going on right now is that third parties who want

access to data – and by third parties I mean those who are not involved in the contract between the registrant and the registrar, the person that is facilitating their domain name, and the registry, a processor down the road that actually makes it happen. Right?

So all other parties are third parties from a data protection perspective, and although they as stakeholders in ICANN, they present themselves as stakeholders who have an interest in the data. So most WHOIS exercises have started with a listing of all possible useful purposes for WHOIS data, or use cases, as they're called. As I say, there are many stakeholders that want the data for market and cost effectiveness purposes. In other words, this is the easiest way to do it, have a free directory.

The cost issues have never really been dissected. We got into a few little fights about cost issues when we were doing the privacy proxy services working group being requestors of accurate data, the real registrant behind the proxy, wanted registrants to basically serve documents for free. Well, that doesn't happen in the meat space, why should it happen in the Internet space?

The technical possibilities have advanced since the first WHOIS protocols were developed. So a revision of this material is overdue anyway so that we can see what's possible with today's specifications, namely RDAP. The value-added services, as I say, they have arisen and they take advantage of free data. And I think it's worth noting here– and I speak as a former government person, so I'm not speaking on behalf of any government, I'm just noting that I did spend quite a bit of time working on some of these – they have been somewhat stymied in the

negotiations with the cybercrime treaty to speed things up and exercise the [inlet] process.

There were very real problems in international harmonization of laws and in getting data cross borders. It's a well-known issue. But the solution to that, I would submit, is not ICANN creating a private sector repository where everybody can fish. That is just not acceptable under an international law or a human rights law. I'm not very good at advancing my slides here.

Carrying on, access to data versus inclusion, the data uses have expanded over the 20 years of a commercial Internet. Some legally, some illegally. And I don't mean just the ICANN uses, I mean this is a trend that has happened. All laws are difficult to enforce, and data protection law is extremely difficult to enforce, particularly when it relies on the individual whose data has been breached complaining, because they are often the last ones to know.

Discerning what is legitimate processing is also inherently difficult, much more so in the case of ICANN when basically, ICANN has been ignoring the messages from the data protection authorities and just publishing it with no controls. I say no controls. There are some controls in the RAA, but the Contractual Compliance have not enforced them, bulk processing being one of them. In other words, we've had a free-for-all. It's very difficult reining that in now.

[Rights of the registrants] have not, in the opinion of privacy advocates and the DPS, been given sufficient attention. We have tried to get a sort of code, charter of registrant rights, and it somehow got turned into a

charter of registrant responsibilities. There has been far more emphasis on the accuracy of data than there has been on the rights of the individual.

However, that is flipping now with the GDPR, so now the registrants can sue, and not only the data controllers such as ICANN or the registrars and registries, but also the data protection authorities who've not acted to defend their rights. This makes the situation acute. So coming up with reasonable regime for legitimate disclosures is a priority, has to be properly framed according to the parameters of data protection law, and it cannot therefore be built on the fundamental premise of an open WHOIS, which we have heard for the past 18 years is not legally compliant.

So I just want to put a plug in for a workshop that the Noncommercial Stakeholders Group is holding in Barcelona on the Sunday prior to the outset of the meeting, so on the 21st. We are going to talk about standards and how they can assist in setting up an access regime for data. And I would not call it a unified, uniform access regime, but it would help facilitate the job of determining when and to whom data may be released, as opposed to published in an open WHOIS.

So the University of Toronto, with whom I'm associated, I just finished my doctorate last year on why ICANN has no privacy, so anybody wants further information, I can bore you for a full dissertation worth on this stuff. But anyway, we have received a research grant from the office of the privacy commissioner of Canada to look into various standardization activities that could assist in giving controllers and processors the confidence to release data.

I have discussed this at the Berlin group, the international working group on data protection and telecommunications, as an initiative of interest in the light of other standards projects they're looking at and in the light of article 42 of the GDPR. The Berlin group, if you're interested, they have a website and they publish papers that have agreed positions from the international data commissioners on technical issues. And this is a technical issue.

The research project will focus on ICANN WHOIS data first, and then if funded, we will move on to ISP data. And this is an issue where there's been considerable tension and legal battles. As I say, it's very analogous to the ICANN situation.

So here are some of the key questions that we would like to answer and do the research on, and by research, I will have a PhD student doing an analysis of what standards are already out there in the various areas, IETF, ISO, and how they might be applicable in this situation. So, first question is, what due diligence does a data controller have to do before releasing the registrant data to a requestor? That could be a large consortium of cybercrime researchers, or it could be an individual. Are there standards that satisfy management practices? And I would suggest that there are, ISO 17065 being one of them.

What standards do the requestors need to satisfy in order to become accredited? And basically, why would you accredit someone as, for instance, a cybercrime researcher if you don't know who he is, who he works for, who he shares data with and whether he's meeting accepted management standards for data protection practices, whether he's amendable or accessible to an audit, where the data is held. These are

the kind of questions that the data protection authority is going to ask when a registrar releases data.

And what security standards should ICANN be demanding on any access model? So I'm no expert in security standards, but I'm confident that there are some out there. there's already one for accrediting those who give certifications for websites, that one could be modified or used straight off the shelf to help us on some of these questions.

So the other question is, what can RDAP do to help? It's a very complex – well, not complex, but it's a very articulated protocol now, there's plenty of things it could do without publishing data. It can do discreet searches. So that's basically my presentation. Happy to answer questions, and I included a quick pop quiz here if you want to do the quiz, or go to questions. Entirely up to you, Tijani, I guess. So back to you. Thanks.

TIJANI BEN JEMAA: Thank you very much, Stephanie. Thank you again, because you gave us another way to see it. I am really happy to have you on this webinar, because you gave your – not only what is going on, but also what you are working on, and I think this is an enrichment for this webinar. Now, for the staff, can we please start the pop quiz questions?

ANDREA GLADON: Yes. Thank you. Give me just a moment. We will go back and start with Thomas', and t hen we'll go forward with Stephanie.

TIJANI BEN JEMAA: Okay.

ANDREA GLADON: So give me just a moment while I [post] the questions. Okay, for the first question from Thomas, the fact that I am allowed to collect data legally means that I may also share it. Is that right or wrong? Please vote now.

TIJANI BEN JEMAA: Why I cannot see the questions on the Adobe Connect?

ANDREA GLADON: Let me see.

TIJANI BEN JEMAA: Normally, they are displayed.

ANDREA GLADON: They're not over on the right? You can't see them over on the right-hand side under the agenda?

TIJANI BEN JEMAA: Okay, never mind. We will not lose time on that. So go ahead, please. Repeat the question.

ANDREA GLADON: Thank you. The fact that I'm allowed to collect data legally means that I may also share it. Is that right or wrong? Please choose one answer. And it's over on the right underneath the agenda pod.

TIJANI BEN JEMAA: But how the attendees will answer this question if they don't have the pop quiz on the screen? Okay, we have one hand. Go ahead, Sarah, please.

ANDREA GLADON: Okay, it looks like it is open now.

TIJANI BEN JEMAA: Sarah, go ahead. You are muted, I don't hear you. Sarah Kiden, do you want to speak?

ANDREA GLADON: Okay, it looks like we have three people who have answered the question now.

TIJANI BEN JEMAA: Okay. Now it's okay.

ANDREA GLADON: So 83%, five people have chosen that this is wrong, that is incorrect. Is that the correct answer, Thomas?

THOMAS RICKERT: That is the correct answer, yes.

ANDREA GLADON: Great. We will go on to the next question. Give me one moment. Okay, the next question, if the EPDP is not completed within a year of the adoption of the temporary specification, the temporary specification will become a consensus policy. Is that right or wrong? Okay, and we have received six answers, eight now, and it looks like most of them are choosing "wrong." Is that the correct answer, Thomas?

THOMAS RICKERT: That's the correct answer. It does not become the consensus policy automatically.

ANDREA GLADON: Great. And for Thomas' last question that is now open, contracted parties send data to the EBERO. Is that right or wrong? Please vote now. Okay, it looks like we have six people who have participated, and 66% have chosen "right." Is that the correct answer, Thomas?

THOMAS RICKERT: Unfortunately not. The contracted parties do not send data to the EBERO. It's retrieved from the escrow agent and then passed on to the EBERO.

ANDREA GLADON: Thank you. We will move on to Stephanie's questions now. Stephanie's first question, escrow data is stored in the U.S., and the contract says only ICANN can access it. Law enforcement agencies cannot access that data. Is that true or false? Okay, we have nine people who have answered, and 77% have chosen "false." Is that correct, Stephanie?

TIJANI BEN JEMAA: Stephanie? You must be muted. Star seven to unmute.

STEPHANIE PERRIN: "False" is the correct answer.

ANDREA GLADON: Great. Thank you. I'll move on to the next question, and that poll is now open. Cybersecurity investigators need the name of the registrant to do data analytics. Is that true or false?

TIJANI BEN JEMAA: But Andrea, you have only one place, one – where you put true or false.

ANDREA GLADON: Oh. Yes, I apologize. Yes, I'm sorry, I messed that one you. Stephanie, could you give us the answer for that one?

STEPHANIE PERRIN: It's "false." They can do data analytics with all kinds of things, including an encrypted identifier, a hash, and all the other data that does not include the name.

ANDREA GLADON: Thank you. For the next question, there is no current process to permit LEAs to search WHOIS anonymously for serious crime investigations. This is why it has to be open WHOIS. Is this true or false? Okay, we have nine responses, and 66% have said "false." Is that correct, Stephanie?

STEPHANIE PERRIN: That's the right answer. There's new research techniques on the go at the moment that could allow law enforcement to have secure, anonymous, untraceable access to do their searches.

ANDREA GLADON: Thank you. And for the next question, once a data controller releases data to a third party, they no longer have liability for what happens to that data. Is that true or false? Okay, we have ten participants who answered this one, and 60% have said "false." Is that correct?

STEPHANIE PERRIN: "False" is the correct answer. Depending on the circumstance under what you release the data, you may still be liable for what happens to it. In other words, if you didn't do due diligence and you, like for instance Equifax, sold the data to a criminal identity theft ring, you might be found to be liable.

ANDREA GLADON: Thank you. And for the last pop quiz question, there was no data protection law when ICANN was born in 1998, the GDPR is a new thing. Is that true or false? Okay, we have ten participants who have answered, 11 now, and 72% are saying "true." Is that the correct answer?

STEPHANIE PERRIN: No. Actually, the correct answer is "false." The directive 95/46 passed in 1995 and had a deadline for European data protection law to meet the standard of the directive by 1998. Now, some European countries have not revised their laws, and I don't have a completely accurate count on how many laws were in place, but at least 20 in the European Union area by 1998, and there were other data protection laws in place such as Hong Kong. Canada had passed its private sector law – tabled its private sector law. So this notion that the GDPR is a new thing is fundamentally false. There have been very few changes in the actual interpretation of the provisions between the old regime and the new regime.

TIJANI BEN JEMAA: Thank you, Stephanie. I'd like to ask you why so far, or until 25 of May, all the WHOIS – the thick WHOIS was public, [while there is those data protection laws and in force?] I don't understand.

STEPHANIE PERRIN: Pardon me while I just mute my speakers again or I'll get an echo. It's an excellent question, and one I asked myself when I did my dissertation. It shows a failure in enforcement on the part of the data protection authorities. It also shows the reluctance to go after ICANN. I think there's an acceptance that it was ICANN setting the rules, and as long as the U.S. government and ICANN basically rebuffed any attempts to enforce European data protection law, nobody was going to try to sue anybody in California for this. And I think there were bigger fish to fry, frankly, when it came to [transporter] enforcement.

So I think that that was probably part of the reason there were no enforcement actions. I have spoken to data protection authorities, and they basically said, "Why should I – I'm trying to find the right word here – penalize our local registrars for complying with ICANN's requirements and let American companies go scot-free?" And that's an excellent question. And so of course, a German data protection authority could have gone after a German registrar a decade ago, easily, but why would you do that and penalize your own companies and open up the market to those who do not have data protection laws?

TIJANI BEN JEMAA: Okay. Thank you. So Andrea, it was the last question, isn't it?

ANDREA GLADON: Yes, that's correct, we have no further pop quiz questions at this time.

TIJANI BEN JEMAA: Okay. Thank you very much. So now, I open the floor for questions for Thomas and Stephanie. So please, raise your hand if you want to ask a question. I need your question. We managed to have 20 minutes more on this webinar so that you can ask questions. No questions? So I will ask a question for you before you want to ask your question yourself. Thomas, do you think that there is a chance, there is a possibility that in these few months, the ICANN community will manage to have a consensus on all those contentious issues? All of them, we have different point of view inside the community, and the community are strongly standing by their position on them. So, do you think that we'll manage to have something at the end of – by 25 of May?

THOMAS RICKERT: Tijani, I guess that's an excellent question. The ICANN community is not known for being particularly fast when it comes to policy development. However – and you know this better than many, you know as one of the co-chairs of the accountability cross-community working group that whenever there's pressure on the community, whenever there's a deadline, then the community can do remarkably well. And I think [the incentive] for this group to come to consensus by the deadline and have this done within a year is that the temporary specification will be out of existence after that, and that will lead to fragmentation of the marketplace more than we see today, and that will probably lead to a situation where certain contracted parties will use an even more restrictive approach to GDPR in order [inaudible] to protect themselves.

So I guess that those who are not happy with the temporary specification at the moment mostly look for the temporary specification

to be more liberal or the outcome of the policy process to be more liberal so that more data [inaudible]. I think they will only achieve that goal, if at all, if there is consensus on such approach. Also, I think that if we mange [inaudible] group to work based on [inaudible] methodology and not politicize the discussion, I think we can pull it off. I'm a helpless optimist, as you can hear, but I'm a huge believer in the ICANN community and what it can do, and so I think that we can do the job [inaudible].

TIJANI BEN JEMAA: Lucky you, to be so optimistic. I really hope that we will reach some kind of consensus before the deadline. I have one hand now, Auwal. Excuse me, I cannot read well your name. Go ahead, please. Auwal Tata, I think. You have the floor.

ANDREA GLADON: Please check your mute button. It appears that your line is open.

TIJANI BEN JEMAA: If you are using the phone bridge, star seven to unmute.

ANDREA GLADON: He is only on the AC line, so for some reason those on the phone bridge cannot hear him.

TIJANI BEN JEMAA: So what is the solution?

ANDREA GLADON: Only the people on the AC will be able to hear him at this point, there's not – unless he wants us to try to call out to him. If he wants to provide the number, then we can call out to him. But for some reason, those on the AC can hear him, but not those on the phone.

TIJANI BEN JEMAA: Thomas and Stephanie, are you on the AC room? Do you hear the question?

THOMAS RICKERT: No, I'm taking the audio from the audio bridge.

STEPHANIE PERRIN: I am now on the AC room.

TIJANI BEN JEMAA: Okay. So can you hear the question, Stephanie? Or perhaps if you can –

ANDREA GLADON: Go ahead and ask the question again, [if] Stephanie can hear you.

STEPHANIE PERRIN: Could you just repeat the question again? Thanks.

ANDREA GLADON: We do have the operator trying to dial out to him. I'm not sure if Stephanie is able to hear him.

TIJANI BEN JEMAA: Okay. Can he type his question on the chat? Okay, is there any other question for Stephanie and Thomas? Okay, waiting for other questions. Oh, he's typing his question. Okay. So you have the question on the chat.

ABDULKARIM AYOPO OLOYEDE: Hello.

TIJANI BEN JEMAA: Interpretation –

ABDULKARIM AYOPO OLOYEDE: Hello.

TIJANI BEN JEMAA: Yes. Go ahead. Abdulkarim, are you the one who has a hand up?

ABDULKARIM AYOPO OLOYEDE: No. I'm just on the phone bridge.

TIJANI BEN JEMAA: Yes. Moment, please. One second. So now you have the question on the chat. If data protection rules have been in existence long before GDPR, then why –this is my question – is it that it wasn't effective? So this was the question I asked, and Thomas – Stephanie, I think, answered it. The answer is that it wasn't enforced. And for example in Canada, the data protection commissioners said that they don't want to penalize their registrars and let the American registrars work without restrictions. This was the reason. But now with the European law, new law or new regulation, everyone has to comply with it if they want to serve European people or serve residents in Europe. I think this is the answer. Okay, now we have Abdulkarim. Abdulkarim, go ahead, please. Abdulkarim, go ahead.

ABDULKARIM AYOPO OLOYEDE: Hello.

TIJANI BEN JEMAA: Yes, go ahead.

ABDULKARIM AYOPO OLOYEDE: Can you hear me now?

TIJANI BEN JEMAA: Yes, I hear you very well.

ABDULKARIM AYOPO OLOYEDE: Okay. Thank you so much. I want to first of all thank the presenters for a wonderful presentation. But my question is, why did it take ICANN so long? [inaudible] similar to the other question. If we've already known about GDPR for some time now, why has it taken ICANN so long to come up with a permanent solution?

TIJANI BEN JEMAA: Very good question, but you know that since the beginning, the discussion about the WHOIS data didn't stop, and we had always working groups on it. And it was especially because there is two values that are opposed, the value of data protection or privacy, and the other value is transparency. So the community inside ICANN couldn't find the consensus about that.

And I remember that the current CEO said in one of the sessions in one of [the] ICANN meetings that GDPR is an opportunity, is a good opportunity for ICANN. And I think he's right, because if we didn't have the GDPR, we would never have a consensus about the WHOIS, registrants data and how to protect them, at what level we have to protect, what we have to protect, what you don't have to protect, etc.

So this is why ICANN didn't come up with its own, if you want, way to solve this problem. And now that there is regulation, binding regulation, ICANN is obliged to comply with it. There was before binding regulations, in Canada for example, but it wasn't enforced, and that's why ICANN didn't care about it. Have I answered your question? Thomas and Stephanie, do you want to give more information about that?

THOMAS RICKERT: Stephanie, you go first.

STEPHANIE PERRIN: Just to add to that by saying nobody's ever proposed 4% fines before, and that is [what has focused the minds,] and it's very clear that the contracted parties are going to be paying those fines, so they are no longer collaborating with the third-party interests who want to have access to the data. So I think that's it in a sentence, but I'd be interested to hear what Thomas says.

TIJANI BEN JEMAA: Thomas?

THOMAS RICKERT: Thanks very much. Thanks for the question. I guess we have a couple of factors that make the system change or that might make the thinking change. First, you have [inaudible] Now [inaudible] 20 years, we didn't have activists that would dare to stand up against companies such as Facebook, but [inaudible] Stephanie mentioned, the invalidation of the safe harbor by the European court of justice, and that triggered [inaudible] an Austrian lawsuit [inaudible] the way Facebook treated him. And therefore, he took it all the way up through the [inaudible] and got the safe harbor abolished. And now [inaudible] and Stephanie also alluded to that, we have this possibility for activists or [inaudible] data subjects to go after the [offenders if they are enacted.] Right? So there's now a different pressure on data protection authorities to

actually [inaudible] that are brought to their attention. GDPR [inaudible] and data processors outside the EU [inaudible] And that means that now not only [inaudible] have to comply with the previous data protection laws the directives, but our companies globally that are working with Europeans or offering their services to Europeans are facing these hefty fines. And I think this combination makes it worthwhile for a lot of [inaudible] to actually consider to become compliant. [inaudible] with respect to .eu or .africa. And .eu, since they are targeting the European market, they have to be fully GDPR compliant, and for other CCs that are outside Europe, if they choose to market their TLDs to European registrars or [registrants, they're now facing] the European market, they [might] also need to be compliant based on the criteria [inaudible] mentioned earlier.

TIJANI BEN JEMAA: Thank you, Thomas. I'd like to highlight or throw emphasis on the fact that as Stephanie said, now that there is fines, and very important fines, against people who will not comply with GDPR, made it effective, really effective. Perhaps the other laws, such as the Canadian one, perhaps they don't impose such fines. Okay, other questions? Dave.

ANDREA GLADON: Tijani, we are now 20 past the hour.

TIJANI BEN JEMAA: Pardon? Oh, okay. We will take this question. Dave. Dave? The last question. Dave, you are muted. Star seven to unmute.

ANDREA GLADON: I believe that Dave is not on the bridge, so he is only in the AC, so he's going to need to type his question.

TIJANI BEN JEMAA: So Dave, can you type your question in the chat if you are not on the – okay, I think he's typing now. And this is the last question. And I would like to thank very much the interpreters. We will finish now, just after this question. Okay. If it is too long, Dave – okay, thank you. So since Thomas mentioned that the temporary specification is for a period of [90] days and four times can be extended, and the worst case scenario – it is not finished, the question. Yes, Thomas said that. The temporary specification are valid for [90] days and they can be extended several times, until one year. The total is one year. Not more than one year. Is it that your question, Dave? Okay.

Okay, and for your information, Stephanie gave her e-mail address on the chat, and you can ask her your questions at any time by e-mail if you have other questions. And Thomas also gave his e-mail address on the chat. What will happen if – yes, this was answered by Thomas, but I will give him the floor to answer it. Thomas, he's asking if we don't reach the consensus and we cannot have the policy at the end of – by 25 of May, what will happen?

THOMAS RICKERT: Then the temporary specification is not valid any longer, it has not been followed or implemented by a contracted party, and since ICANN

cannot force the contracted parties to operate in contradiction to applicable laws – that would include GDPR – there will be a vacuum, because then every contracted party would basically do what they think is required to be done in order to be GDPR compliant.

TIJANI BEN JEMAA: And this is what we call fragmentation. Thank you very much, Thomas, and thank you all. We have to close this webinar because we are out of time. I'd like first to thank our two presenters, Thomas Rickert and Stephanie Perrin. Both of those presenters, for me, are more passionate than professional. They are professional, of course, but they know very well the subject and they are passionate about it. And that's why I invited them.

Also, I would like to thank the interpreters for the overtime, and our staff, everyone, and you who attended this webinar. I hope you'll have other questions to ask Thomas and Stephanie by e-mail, and this webinar is now closed. Thank you very much.

ANDREA GLADON: Thank you. This concludes today's conference. Please remember to disconnect all lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]