EVIN ERDOGDU: Welcome to today's call, the EURALO webinar on general data protection regulation (GDPR) on Monday, 19th of February 2018 from 19:00 to 20:30 UTC. Just as a reminder, we will not be doing roll call today as it's a webinar, but if I could please remind all participants on the phone bridge as well as computers to mute your speakers and microphones when not speaking and please don't forget to state your name before speaking not only for the transcript, but also for the real-time transcription purposes.

Also, at the end of the call, we will be having a user experience part, which will be a several-question survey. I will change the AC room format in order for everyone to answer the survey. It'll take about five minutes to complete. Thanks so much, and back over to you, Olivier. Please begin.

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Evin. I'm the chair of the European At-Large Organization (EURALO). We've got a webinar today that thankfully was quite widely broadcast and publicized, so we have a good turnout for this webinar. We also have a scribe captioning pod that should provide for immediate transcription of what we are saying. So, one of the things that I would ask when people do speak afterwards is to identify themselves when they start, so as to be able to have good, reliable transcripts on today's session.

The idea for a webinar on GDPR is something that you might not see as being very original at the moment. There are quite a few webinars that

we've seen over the past few weeks. I know that we are going to see further webinars on this topic in the forthcoming weeks and perhaps even months.

The regulation itself was passed a while ago, but the enforcement date as listed on the European Union's GDPR, eugdpr.org website, enforcement date seems to be the 25th of May, 2018. So, we really are looking at the final countdown before things started getting enforced.

No doubt Thomas Rickert from the ECO Internet Industry Association will be able to provide us a good update on this, and perhaps even a view from the registrants or a commercial organization's point of view as a whole.

We have also Pierre Bonis, from the AFNIC dot-fr registry. That's the country top-level domain for France and he'll be able to provide us with some details and perhaps a perspective from a ccTLD (country code top-level domain) points of view.

Michele Neylon is also joining us on the call today. He runs Blacknight Solutions, [inaudible] domain, a longstanding ICANN participant and very active in the Generic Names Supporting Organization. He will be providing us with a perspective from the European Registrar and business point of view. In fact, Michele has been very active in complaining to ICANN about some of the problems of ICANN's contracts over the years with ICANN not doing very much in response. So, perhaps he will be able to provide us with a bit of insight into this. But, certainly, European registrars are probably the first affected or the most affected of all the registrars out there.

Then, we have Atihna Fragkouli from RIPE NCC, RIPE Network Coordination Center. The RIPE NCC is the European regional Internet registry. Regional Internet Registry is the distributor of Internet protocol addresses, IP addresses. And of course whoever says registry also means running a very, very large database.

So, the idea for such a webinar, as I said, there's so many other webinars on GDPR recently. The idea for such a webinar on practical implementation of GDPR from all of these different perspectives came from a sort of side brainstorming session that several of us had – several of us being people from the members, and also members of the board of EURALO, had during the Internet Governance [FIRM] event in Geneva late last year and there was an Internet Society party that took place. We all had a glass in our hand and we started thinking about what EURALO could do to really help in various topics. GDPR was the first one that came on the table. The idea was to say, well, look, we've got all these theories and all these things about what is the GDPR and how is it likely to affect people and so on. But, very little of the actual practical implementation. What does it mean on the ground?

As we all know, in theory – theory is the same as practice. In practice, it is not. So, now that we know that we're in for an interesting ride [inaudible] looking forward to hearing everyone on the call here. I think there's somebody who needs to mute themselves, perhaps. Anyway, I don't want to ramble on for too long. You've not come here to listen to me. You've come here to listen to our four panelists, so I'm extremely pleased to be introducing Thomas Rickert to you and to hand the baton over to Thomas who I understand has got a small presentation for all of us. So, Thomas Rickert, you have the floor. Thank you.

THOMAS RICKERT: Thank you very much, Olivier. This is Thomas Rickert speaking, representing ECO, an Internet association with more than 1,000 members from 70 countries around the world. We've been quite active in the GDPR discussion.

As you may or may not know, ICANN has been quite silent on this topic. They haven't really suggested how the GDPR topic can be tackled, and then ECO stepped forward and came up with a [data] model that could be applied to the gTLD space.

I have to say two things as a word of caution. I have a little bit of a cold, so I hope that my voice is not going to let me down. So, if I start coughing, then I think the next speaker should just take over.

Other than that, and that's my [inaudible] in my time zone and could there be any better way to spend an evening than talking about legal stuff and the GDPR? So, let's dive just right into it.

I should say that – and you will have noted from the agenda – that we have changed the speaking order. I am going to introduce very superficially, very briefly, to you some of the main idea, some of the basic principles, of the GDPR, which are applicable to everyone. But, then, you will hear Pierre from dot-fr, from [APNIC] and then you will hear Athina from RIPE. There's a little bit of caution to be applied because what's true for the gTLD world is not necessarily true for the ccTLD world or a database of IP addresses because the policy is set up, the contracts set up, is completely different or it can be completely

different and that can lead to a different legal assessment and different impact of the GDPR.

So, Olivier mentioned earlier, but just to recap, it will kick in – the GDPR, that is – on the 25th of May and it will enter into [inaudible]. But, on the 25th, it has already been published two years back. So, it's not really news and it will be immediately applicable on that day. There are folks who are confusing the concepts of [directives] and regulations, and while regulations have immediate effect, [directives] have to be transformed into national law. So, that's one of the major distinctions. So, after May 25th, we should all be compliant.

The goal of the GDPR is to regulate data protection [inaudible] the EU to give EU citizens better control over their personal data and regulate how controllers may use personal data. On the other hand, should ensure free flow of data within the EU and to regulate the export of personal data outside the EU.

Now, that [inaudible] quite some concepts which are in the GDPR. First of all, it's personal data. So, if you are an individual, if you are registering a domain name, GDPR will kick in immediately. If you are a company, then you need to be a little bit more cautious because while a lot of folks, even particularly outside the EU, think that corporate data can never be personally identifiable data, that is not true.

Corporate data, company names, can be PII as we call it – personal identifiable data – if it allows for the identification of an individual. Therefore, just opening up two buckets, one for private users and one for company users, doesn't do the trick. And therefore there is some

issues and this is why we have suggested that all data should be treated the same in order to avoid the risk of corporate data, which actually is personal data being publicized without having a legal basis for it.

Let's look at some of the main themes. There are increased transparency requirements. That's important to users. You, as a user, as a registrant, need to be told exactly what's going to happen with your data. The documentation requirement, information requirement, and the operators need to be able to prove how they [inaudible] the data and what they did with it. There are increased data security requirements for operators. There are increased accountability requirements, such as to report certain data breaches. There is the right to be forgotten.

So, you can say to an operator that you don't want them to have your data anymore. Then they actually have to delete it. Certainly, this will be overridden where there are statutory archiving provisions, for example. So, your data will not necessarily go away entirely, but a legal basis is needed for the data to be retained. There is the right to data portability. Then we have two concepts, privacy by default which means that all systems need to be set so that they have minimum impacts on your data protection. So, no pre-tick boxes for consent and other things. You have to set the settings and make them less harsh than they are [beginning].

Then, privacy by design means that you need to build your systems so that they actually comply with the principle of data minimization, so that no more data is collected and processed than actually required to

fulfill a contractual purpose or within the boundaries within another legal basis.

So, to sum this up, you as a registrant have certain rights based on this. You can actually go to a registrar or where the registry has your data and go ask them what data they have about you. You can ask them to rectify your data, and if they are doing something wrong, you can try to get relief for that and you can go to the authorities and complain about an operator. And if the authority doesn't take action, then actually you can take the authority to court for inaction.

That leads to sort of what some call a vicious circle whereby [inaudible] operator do not get compliant in time. Suddenly, users can go and force the authorities to take action against the operator.

Let's try to familiarize ourselves with some principles of lawful processing. First of which is consent. So, if there is the free will by data subject to consent to processing of data, that's perfectly possible to use as a legal basis. But, this consent has to be informed and it must be freely given. So, there's the so-called provision of bundling, according to which an operator, a registrar, can't tell you, you can only have a domain name if you consent to the publication of your data via public WHOIS directory. So, that would be wrong.

This is why we don't focus on consent-based processing, although it is possible. You can, however, do what is required to be done to perform a contract. My typical example is if you are an online bookshop, certainly you need to know to what address to ship the book. So, you can have the data to fulfill the contract. Then, performance to comply with the

legal obligation. So, if law enforcement authorities that are in your jurisdiction ask you for disclosing data, then you can review data to comply with the legal obligation to disclose data.

Let's move to the next slide. Then, there's processing in the public interest. But, for that to happen, you need to really have an official authority or you must have invested with a public function and the European Commission has now mentioned that 61E, but they have not really specified that data can be processed by ICANN having this public mandate, if you wish. So, that's something that we need to build down on and ask the authorities to provide some guidance on.

The last one is legitimate interest. So, if you think you have a legitimate interest to process data and that can be to reveal it to the authorities, to law enforcement, to IP lawyers and others. Then, what happens is that you can't just do it. You have to think carefully about whether the legitimate interest is present or not. And if you think you have that legitimate interest, then the data subject can still say, okay, but I think that my interest in keeping my data protected outweighs the legitimate interest of the controller. Then you start – when such objection comes in, then you need to start a balancing act. And at the moment, the GAC as well as the European Commission are asking to keep the WHOIS as open as possible and keeping it open or more or less open or create little hurdle would automatically lead to the notion that the legitimate interests of IP lawyers, government would always outweigh the rights of the data subject. I'm not saying that this is perfectly impossible, but we need guidance from the authorities to help with it.

I will be done in a moment, but this chart shows you contractual relationships that we're working with in the gTLD world. So, we have a registrant [inaudible] registry through a reseller or directly with the registrar. Then the [inaudible] transmits data to the registry. But, in case of registry failure, you have the emergency backend operator, which you see at the far right of the slide, the bureau that can gain access to data. You have different escrow agents for registries and registrars. Then you have ICANN prescribing the processing of certain data. Then you have WHOIS customers that want to get access to that data.

All of these processing steps need to be analyzed. At the moment – and I'm sure that Michele will join me in saying so. At the moment, ICANN has not yet come up with a robust explanation of the legal argumentation, the legal grounds, for all this processing that is required. We hope to have contributed to this discussion with your, as we call it, ECO GDPR domain industry playbook which you can find amongst the community proposals on ICANN's website.

But, I think what we should expect probably is that the current collection of data collecting registrant data admin [c] data, tech [c] data, billing [c] data might not be compliant with the principle of data minimization. So, it is possible that registries, who for example have a local presence requirement or other eligibility requirements might need that data, but then they would need to say so, where for normal domain registration you might only need the registrant. So, we might not see that much of an admin [c], tech [c], or billing [c], particularly since research of registrars has shown that in more than 90% of the cases, the registrant data is identical to the other role context data. So, expect some changes at that front. I think I should pause here and I'm happy to

answer questions when it comes to the discussion part of this call. Thank you.

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Thomas. Thank you for respecting your time and going pretty quickly through the slides, but certainly particularly exciting time that we're going through at the moment. You mentioned Pierre Bonis and the country code top level domain operator at ccTLD. Well, Pierre is running AFNIC, the dot-fr registry and he's now next in line to tell us about the GDPR from the European Country Code Top Level Domain operator's point of view. Pierre, welcome. You have the floor.

PIERRE BONIS: Hello. Thank you very much [inaudible]. Do you hear me well? I hope so.

OLIVIER CRÉPIN-LEBLOND: Very well, indeed.

PIERRE BONIS: So, first of all, thank you, Olivier and a big thanks to ALAC who have organized this webinar. I think it's very useful and I'm very happy to participate. I'm going to go through very quickly the first … I have two small presentations. One that is dedicated more to the ICANN context and the other one to the FR context, because as you said, I'm here as the CEO of a ccTLD that we are also involved in the ICANN discussions, not only through the ccNSO but because I think it's also running as a backend registry some gTLDs.

I'm not going to go through what Thomas has explained very, very brilliantly before about the main principles of the GDPR. I will go directly to the content because it has been said before, and to the access, but to the personal data disclosure.

The funny thing is that today a lot of players within the ICANN ecosystem are upset or let's say they fear that being compliant with the GDPR is going to make a huge difference for them and they will have to work a lot on their own information system to make it compliant.

That's funny because we did exactly the contrary. When we [inaudible] it trying to be a backend registry for gTLD, it could have been much more simpler to copy the dot-fr system to the gTLDs, but we didn't have the rights to do it because by contract with ICANN at this time, and today at the moment where I think also it was not possible to be compliant with the personal data protection laws, so we had to work on an automatic system from the dot-fr we were running for more than 20 years. And we did it, so I'm very sure that the big players around the big registries will be able to do it also. I think there is a necessity to implement the GDPR in a [inaudible] and I'm sure that Michele will agree on that, so we don't have different solutions from different registries. But, at the end of the day, the developments that are needed are not so huge from our point of view.

So, the main thing to me and to AFNIC is, as [inaudible] understood, not really in the change in the system that we have to do. To us, the change in the system is fairly simple. It's just hiding the personal data from the natural users and maybe referring to what Thomas said before. We think, in our interpretation, that has been checked with the French data

protection authority is that the personal data that is sent by an enterprise may be personal data, but it's in the remit in the business. It's not in the remit of the registry, which means that when you talk about data that are not from natural persons, they are not covered by the GDPR.

So, at the end of the day, what do we hide and what do we have to hide from public availability? The name, the first name, the surname, and the address and the telephone number, and everything that is strictly personal data. This is very simple to do that technically.

What is not simple on the paper is to make sure that once you have done that, you still have the opportunity to give access to this data to people with legitimate interests. I may say that we haven't got an automatic solution for that, but we have done that in the dot-fr since more than ten years now manually. Dot-fr is more [inaudible] domain names, so it's not a very big extension, but it's not a small one. For those who are not very familiar with France, you should know also that we have a very strong IP industry in France and a very strong industry [linked] with luxury products, so they are very interested usually trying to fight cybercrime. And we have an average of a little bit more than 400 requests per year that are all checked manually and this is done by one woman who is not doing that all day, of course, and who is doing a lot of other things than that.

So, we think that the manual approach to asking for accessing to personal data is a good approach, and we think that the important thing is to explain that, accessing to the personal data of a registrant is something that cannot be automated because it's, in a way, restricting

the right of the registrant itself. So, you must have a good reason to access personal data, that however, you should not have to access.

So, I don't know how it can be automated and if it is automated, in a way, you weaken the rights of the registrants and the GDPR is all about enhancing the rights of the registrant and not weakening.

So, we have some other issues that we have not exactly found a solution for now. It's the period of retention of the personal data. Of course, if the domain is active, as long as the domain is active, the retention should be okay. But, how long do we retain the old data of an active domain name? This is something that is not very clear for us. The escrow data, what do we have to do with our suppliers of escrow, which I'll remind you is an obligation of the ICANN contract.

So, these things are not perfectly clear now to us as a backend registry and also as a ccTLD registry because of course the retention is an important thing for a ccTLD and the escrow is a good practice that is used also by the dot-fr.

So, that's why I say that the impact somehow more on this kind of gray part of the GDPR done on the [inaudible] path that is [obvious], just hide the personal data in the root and that should be enough at the very beginning.

That was the first part of the presentation. Maybe I'm not going through the FR part of the presentation now because I'm going to be too long, but I just wanted to share something with you, and especially because as users I think in ALAC and also as the stakeholders in the ICANN system, you may wonder if there is going to be different way of

implementing the GDPR. We all know that the ICANN management, the ICANN leadership, has offered three models for discussions. It's a little bit unclear for us if these models have to be implemented of this model, if one chooses, has to be implemented before May. It's a little bit unclear to us if this obligation is compatible with the current contract that ICANN has with registrars and registries.

Nevertheless, even if it's a little bit … I mean, we are a little bit puzzled, but what we understand, which is there is a model that has to be implemented in less than three months and we don't believe that this is something that is compliant with the ICANN rules. The idea behind that we think is that ICANN tries to make sure that there will be a global solution for handling the GDPR and that will be easier for the registrants to understand their rights, whether they are on the dot-com, dot-fr, or dot-paris and it will be easier also for the registrars to deal with it.

But, I have to share a last point with you is that the GDPR is implemented. Of course, it's a basic set of rules, so it applies the same way in all the European countries. But, at the same time, the personal data protection laws that have been passed before the GDPR has [inaudible] some laws that are related to the ccTLD registries. Not all of them, but most of the ccTLD registries, operate under national laws and sometimes these laws are specified some very, very precise things about the protection of the data, of the personal data. And as long as these laws have not changed, the way that the GDPR is going to be implemented by various ccTLDs [inaudible], may be different from one ccTLD to another.

I will end with that. The model that AFNIC is not promoting, but the model that AFNIC is working on is compliant of course with the French laws that separate very clearly that the registrars are responsible for their data and the registry is responsible for [inaudible], which means that we are in the model where registrars are data responsible, registry is data responsible, and there is not a contractor or subcontractor model that may be used by some other ccTLDs or may be used also in the ICANN model, which means that the diversity of the model is not going to end in the blink of an eye in May. We will still have some differences in the way that we implement the GDPR, or at least this is what I expect.

At the end of the day, the diversity of the implementation, as long as all the implementations are compliant with the law, reflects maybe the diversity of the TLDs themselves, the values they carry, and the countries sometimes they represent and I don't think this is a bad thing. So, I think with that, I will finish my presentation and maybe allow more time for questions and answers. Thank you.

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Pierre. Should I say [inaudible]. It's quite a complex environment here and certainly this is quite exciting. Where are going? Basically. Without any further ado, let's go over then to Michele Neylon, who is with Blacknight solutions hosting [inaudible] and domains. He runs the registrar and has run a registrar for a great many years and has been very vocal on these issues, so I hand the floor over directly to Michele.

MICHELE NEYLON: Thanks, Olivier. Hopefully, everybody can hear me okay. If I speak too quickly, please let me know, as I'm Irish and I have an awful habit of speaking about a mile a minute.

So, I'm not going to spend too much time talking about WHOIS and the ICANN piece because the other panelists have spent a lot of time talking about that.

The perspective I bring on this is slightly different. I'm looking at this more from the approach of a company that operates online and needs to deal with GDPR across all lines of their business.

If you look at the first slide there, you can see obviously it's promotional. We offer domain names. We offer hosting. We offer e-mail. We also provide connectivity for businesses. We've recently branched out into offering connectivity to businesses in terms of DSL lines and all those kinds of things. We offer digital certificates. And each and every single one of those things has to be dealt with in light of GDPR.

So, if you look at the next slide – you all have control there. What we've been doing over the last about 12 months or so is going through all of our internal systems, our internal policies, our processes and trying to work out, first off, exactly what data we have and why we have it, and do we actually need to have it?

For example, any business will probably have employees. In our case, we've got about 40 or so. We've been in business for 15-plus years, so

over that time, we've had employees who have left the company. As we went through this entire process, we discovered that we had information about former employees. As other speakers have mentioned, you do need to keep certain information for regulatory reasons. In the case of former employees, for example, we are often contacted by people asking us to confirm that somebody actually did work for us.

We discovered we had way too much data. We had information related to former employees that was no longer pertinent and we had no reason to keep it, so we dumped that.

But, when we're looking across the rest of the business, again we're looking at it in terms of where are we collecting information? What information are we collecting? Why are we collecting it? Do we need a reason to collect it?

Look, I'm not a lawyer. I'm not going to talk about various citations and everything within the legislation. But, essentially, the way we've looked at it is one of following the data and just trying to see if we actually need it, because from our perspective in terms of risk, and that ultimately as a business is what we're interested in, what we're trying to do is trying to work out where the risks are and try to both document them and then address them as best we can.

I think Thomas did mention about corporate, when you're dealing with corporate, how that can also involve personal information. In our case, we have that going both ways. So, for example, if we have a company who signs up to our services, we have a contract with the company. But,

in the course of doing business with these companies, we will end up collecting information related to their employees. We end up sometimes with mobile phone numbers, we end up with e-mail addresses. And sometimes that information is no longer needed, so we have to [inaudible] way of seeing, first off, what we have; and secondly, how we deal with it.

Looking across the full range of products and services that a company such as ourselves offer, we've been going through it in terms of trying to work out, as I said, which risks exist, where they exist, and what can we do about them?

So, if you look at the [inaudible], I talk about mapping risks. There's a difference between a risk that is known and a risk that is controlled. I might know about a risk, but it might be outside my control, which of course makes things quite difficult.

Then, looking at it in terms of timelines, as been said by the other speakers, GDPR comes into effect on May 25, 2018. Being realistic about it, I know that most of us will do our best to be compliant by May 25th, but there are going to be areas where we know we probably won't be fully compliant. And sometimes this comes down to us relying on a third party to update their processes, update their documentation, etc. It's not a simple, straightforward matter of us deciding by ourselves in isolation how we're going to address it.

So, as a hosting provider, one of the big issues for us is around responsibility for data. We have lots of physical servers, and depending

on the service that is being offered from the servers, the responsibility will change.

So, if you look at the last slide, we've done – it's a draft at the moment, subject to change. You'll see we've put together a kind of draft responsibility matrix, which is just kind of helping us to work out which bits of data are things that we, as a company, should be in charge of? In other words, what we have got responsibility. Which bits really lie with our customers, our clients, and which bits could be what we might call a shared responsibility?

So, if we give you a concrete example, we provide e-mail services on servers located physically in Ireland. We give people access to e-mail addresses. They're able to log in. They're able to set things up. Obviously, we're going to look after the physical security of the servers. We're going to make sure that they are running up-to-date software, the servers, the software all of that is not susceptible to attack of some kind. In a perfect world, DDOS wouldn't happen, when in reality it does.

But, ultimately, the users have the ability to change their passwords. So, we cannot be held responsible if somebody either sets a very, very weak password or prints it out and sticks it on a Post-It Note on their desk. Unfortunately, this happens.

There's other cases where we provide a particular facility to our customer, but we have no ability to see what the customer is doing. we don't want to know.

As a hosting provider, we've been getting a lot of requests from companies, from clients, of all shapes and sizes asking us about how

we're dealing with all this compliance. So, this is where a lot of this [inaudible] again, draft, subject to change. But, the idea being to kind of map out those responsibilities and see who should be looking after what.

When we look at the overall risk and look at the percentage of our business that is linked to a risk, as a primary business as a hosting provider. So, let's just say, using ballpark figures, well over half of the company's turnover is tied up in hosting. Domain names obviously are important to us, but it is a lower percentage.

When I look then at the domain registries that we're interacting with and these kind of interesting cross-border issues, that's when we start to run into some issues. We could go to town on all the issues surrounding how that works with ICANN, but in fact in some respects, the bigger headaches aren't coming from ICANN. They're actually coming from some of the country code operators who are demanding very large amounts of personal information.

So, for example, in some cases, you might be asked as part of a domain registration to people not only proof of your physical address, but you might also be asked to show proof of your identity. We have questions open with several of the domain registries around their handling of that data. So, in terms of the risk of something that does kind of keep me up at night. I think I've rabbited on quite a bit there, so I'll shut up and cede to Athina. Thank you.

ATHINA FRAGKOULI: Hello, everyone.

OLIVIER CRÉPIN-LEBLOND: Can I be heard now? Hello? Okay. Well, it looks like I can be heard now. Thanks very much for this, Michele. Sorry, Adigo did mute everyone and I wasn't quite sure whether I was muted or unmuted, but it looks like I'm not unmuted.

Thanks for this, Michele. We'll go over to Athina Fragkouli from the RIPE NCC. [speaking French] as they started their names. That's the regional Internet registry IP addresses. Totally different angle, but equally challenging problem with the GDPR. Over to you, Athina.

ATHINA FRAGKOULI: Hello, Olivier, and thank you very much for pronouncing our name with the right accent and in the right way. Hello, everyone. This is AThina Fragouli, head of [legal] with RIPE NCC. Well, I'm going to give you our perspective in implementation of the GDPR. We all know my [inaudible] already existing EU [inaudible] come into effect May 2018.

Before I talk about the implementation of the GDPR, I would like to give you some background information about the RIPE NCC. RIPE NCC is a not-for-profit organization. [inaudible] members. It's a membership-based organization. [inaudible] the mandate by the RIPE community to act as a [inaudible] IP addresses in the region of Europe, Middle East, and Central Asia. This registration authority includes on the one hand the operation of the [inaudible] available RIPE database, which might be known some via the WHOIS database that we call the RIPE database. We also maintain some non-public registration information.

This [inaudible] very important for the Internet globally. It's [inaudible] that I have used for the public network and this is essential for the proper function of the Internet. Also, publishing this registration information in RIPE database ensures transparency about the proper distribution of [inaudible] resources.

For a third reason, having the contact details of individuals that are responsible [inaudible] the Internet coordination [inaudible] very crucial in case something goes wrong. So, we understand the responsibility that comes with this role. That's why we are trying to enhance our accountability, which [inaudible].

Now, of course the RIPE NCC is based in the Netherlands. So, for us, the data protection legislation is nothing new. We are already covered by the EU data protection directive.

In 2006, also, the RIPE community showed the importance of having the [inaudible] database in compliance with the legislation. So, it established a taskforce – a data protection taskforce – with a mandate to recommend steps for the [inaudible] implementation of the directive and also to develop [inaudible] RIPE NCC and the legal framework for processing personal data in RIPE database. The outcome of this is that [inaudible] published data protection [inaudible].

So, [inaudible] that the RIPE NCC was involved in 2009, the EU public consultation on the legal framework for the [inaudible] RIPE [inaudible] of personal data. We actually responded to this public consultation with [inaudible] together [inaudible]. In this opinion, we highlighted the importance of having the contact details of operators of the Internet

easily accessible to each other inside and outside the EU because this is crucial for the proper functioning of the Internet around the world. That was our statement.

This leads us today where we're preparing for the GDPR. Now we do have the regulation. Yes, of course we feel that we've been always compliant with data protection legislation, but it's always a good opportunity to have a review of all data sets [inaudible] and to make sure we comply with [inaudible].

In March 2017, we established internally a big project about that, and we are being reviewing then all personal data [inaudible]. We have a project team that consists of two legal councils and the security officers and we get supported by our colleagues from all departments, [inaudible].

We also engage with external legal council and our industry partners, and of course we want to be in contact with … In communication with the live community. We cannot change things without consultation in the RIPE community.

So, where are we so far? We have now a couple of [inaudible] data sets that [inaudible] by the RIPE NCC. And we are reviewing its compliance with the GDPR. Our main areas of [inaudible] for the RIPE database, the retention of personal data, our internal [inaudible] personal data and other RIPE NCC services apart from the RIPE database.

Today, for this webinar, I'm going to talk a little bit about the RIPE database, which I believe is an area of high interest in this group.

So, when we talk about the RIPE database, we first need to look into the purpose of having personal data in the RIPE database. The first is it's essential for the legislation, for the data protection legislation.

When the RIPE community and the data protection taskforce [inaudible] looks into the [model] of the RIPE database, they did define the purpose of having certain data in the RIPE database. They described it in the RIPE database [inaudible] terms and conditions in article three. Among others, the purpose includes facilitating coordination between network operators and [inaudible], etc.

It is so crucial to have this information, this [inaudible] publicly available. When, for example, we have cyberattacks or issues that affect the operations of the Internet, network operators need a quick contact, need to establish a quick contact amongst them. And these network operators have no other direct relation. They don't have a [business] relation. So, the one thing is to look into the RIPE database and check who is responsible for the network that is involved in the problem. So, that is the main purpose for us to have personal information in the RIPE database.

Of course, the legislation requires us to have a legal basis for that. We believe that the contact information of [resource] holders is – sorry, my slides are moving for no reason. The legal basis when it comes to the contact information of the [resource] holders is the legitimate interest of the Internet community. The Internet community must know who is responsible for what IP addresses and [inaudible] network, for the purposes I explained before.

Of course, if the resource holder doesn't want to delegate responsibility, delegate to someone else the responsibility of picking up the phone or to respond to e-mails for such purposes, of course they can have the contact details of another individual, but they must make sure they have the [content] of this individual [inaudible] staff or to someone they have a business relationship with, which can be obtained by this relevant relationship.

Of course, if someone wants to have their personal data removed from the RIPE database, there is a [inaudible]. But, of course, every time contact detail are removed, they must be replaced by the contact details of another individual [inaudible].

Also, we do implement safeguards. We have a limit to the number of personal data queries in the RIPE database, and these limits are defined [inaudible] and here is the link to this policy.

So, as I said, it's very important for us to have a clear commission and [inaudible] with the RIPE community and it's very important for us to show, be transparent, and to show to everyone how we implement the GDPR. For these purposes, we have launched a series of RIPE [inaudible] which is a website we maintain and publish research and blogs and things like that. This is the link to the [inaudible] about the GDPR.

The new article will come this month and it will be about – it will give a little bit more information about the legal basis of the [inaudible] personal data. So, thank you. We also have a webpage that's [inaudible] to the GDPR and here's the link to that.

Thanks. I made it just in time. I'm ready for discussion.

OLIVIER CRÉPIN-LEBLOND: That's great, Athina. Thank you very much. We are indeed now finally reaching the point of our call. We have just under 30 minutes for questions and hopefully for some answers, and for a good discussion to take place on the four excellent presentations that we've seen today from the different angles.

Whilst you were all doing your presentations, some questions did come in the chat and indeed some answers also came. Now, in order to ask a question, you either type it in the chat or you put your hand up by using the little person with their hand up on your Adobe Connect. Make sure that your mic is connected and I'll take the questions in the queue, one after the other. We'll have a mix between the questions in the chat and people who wish to ask their question by speaking to the microphone.

Whilst people are gathering their thoughts after all this viable and exciting data that we've got in front of us, let me just ask a few of the questions that we're asked. In fact, the first one that came on the chat was one from Barak Otieno. The question was: "I'm keen to understand whether GDPR will only affect hosted data or if it affects data in transit as well." [inaudible] immediately afterwards followed up and said, "Well, data in transit is concerned as well if and only if the processor of the transit is able to read and distinguish the data. For example, telecom operators are not concerned unless deep packet inspection is used. But [inaudible], telecom operators are also concerned if they can relate – and IP, I guess – an IP address to an individual.

So, there are several levels of this. I know that Barak Otieno followed up afterwards saying a lot of the African traffic does go via Europe. So, it's interesting to see that angle. I don't know if any of our panelists wish to add to this exchange. Otherwise, I'll go to the next question.

So, then, the next question was, going a bit further down Rubens Kuhl asking, "If the panelists could entertain the question about informing the data subjects that their personal data and by whom. Is this a good idea or is this a bad idea?" Who wishes to answer this? Pierre Bonis.

PIERRE BONIS: Thank you, Olivier. Can you rephrase it a little bit? I'm not sure I understand very well, but I think it's a very interesting question.

OLIVIER CRÉPIN-LEBLOND: It's a question from Rubens asking if it would be a good idea if, for example, you could inform the data subjects that their personal data has been accessed and by whom. So, someone in the WHOIS database is told your data has been accessed by such and such. Is this is a good idea? Is this a bad idea?

PIERRE BONIS: Yeah. Okay, thank you. It's a very, very good question. Personally, I think it should be not only a good idea, but the minimum information you have to give to someone. The fact is that we are not doing that currently when we give access to the personal data to the dot-fr registrant, and especially because some public authorities don't want that the people are informed that they have accessed their personal data.

But, I really think that this is something that we should change and we should have a notification when [inaudible]. Even if we don't say who accessed, at least we should say someone has accessed. But, this is my point of view.

OLIVIER CRÉPIN-LEBLOND: Okay. Thanks for this, Pierre. It's funny to think that in cases of LinkedIn, for example, there is a list and it says who has access to your record on LinkedIn. That's an interesting thought, perhaps, on that. Thomas Rickert, you have something to add to this.

THOMAS RICKERT: Yeah. Thanks very much, Olivier. Since you mentioned LinkedIn, a lot of business networks, social networks, they make it a contractual feature for the data to be traceable. They want you to be able to see who saw your profile, and in many cases, the free version of the service does not allow for such tracking, so you have to pay for getting that information to find [inaudible], for example.

So, if you can make it a contractual feature, then it would be covered by this clause 6.1b that I referenced when I did my introductory presentation.

But, I wanted to give an answer that's not a legal answer, but a practical or political answer. When the GDPR was drafted, there was nobody thinking – at least as far as I'm concerned – about the need of law enforcement. So, when it comes to wire tapping or other areas where law enforcement gets access to data or if you take patent traits or

patent databases or trademark databases where information is made publicly available, there's an analogy used to WHOIS many times these days. For these actions, you have a legal foundation. It seems to be haven forgotten when the GDPR was made, was drafted. And now the law enforcement authorities are waking up, the governments are waking up, very frightened that this valuable resource of information will not be accessible or not be so accessible so easily for them.

This is why they're making these calls about the WHOIS data to be in the public interest, the public policy objectives are being pursued with it. But, that doesn't make a legal foundation. We're looking for the governments who want the data to be accessible to explain to us why or how we can make this work. That's a little bit of a challenge.

The law enforcement authorities have even asked that any access to WHOIS data, maybe gated access or otherwise, should not be disclosed to the data subject in order not to have a detrimental impact on investigation. There's a paper that was drafted under the auspices under the Bulgarian EU presidency with Europol. They explicitly say that WHOIS queries should not be traceable. So, that's the [inaudible] situation that we're facing. I think it's difficult to justify that legally, but since the governments want it, the governments have to explain to us how we can make it work without the contracted parties being at risk of being fined or they need to come up with a legal basis, such as a law to make that happen comparable to trademark databases.

OLIVIER CRÉPIN-LEBLOND: Thanks very much for this, Thomas. I note next in the chat is a question from Eve Edelson from the San Francisco Bay ISOC chapter. The question is with regards to the membership database that the Internet Society has. We wonder how or if GDPR impacts info on memberships like mailing lists and maybe the need to repeat opt-in for this.

Now, I've actually followed this on the Internet Society front. I know that the association management system – the AMS membership database that the Internet Society has on its members is currently undergoing an opt-in test or review where people – and I'm not sure whether it's only restricted to European chapters or whether it's actually worldwide chapters, but people are encouraged or are asked to confirm their membership and confirm their ability to have their details in that database. So, I don't know if anybody else has the answer to this question when it comes to whether this is a worldwide thing or just for the European chapters. But, certainly, the Internet Society is concerned with this, too.

[Athina] you still have your hand up. I don't know whether it's another answer that you wish to provide. No? Okay, you put your hand down.

So, the next question is from [inaudible]. It's a question for Athina. Disclosure to third parties for the purpose of adding value-added services, policing cybercrime in the private sector and defending intellectual property rights is not strictly seeking explicitly envisaged in ICANN's existing WHOIS policy. Although it is implicit by the absence of a privacy policy that protects individuals rights. If ICANN wishes to continue with this implicit policy based on RIPE's experience coming to

understand the GDPR, what do you think that ICANN needs to do to legitimize this?

That's a question for Athina. I think that your mic is not working at the moment, Athina. I think we have a technical problem here. Okay, if I could ask staff to please check on Athina's line because I'm not hearing her. I hope I'm not the person who has dropped out of the call. I can certainly see myself being transcribed, so let's move to the next question in the meantime. Athina, unfortunately we can't hear you, so we'll check with staff. Perhaps your mic has become unplugged or something. The Adobe Connect is sometimes notoriously a bit tricky.

Next is a question from Jim Prendergast. Does GDPR only apply to European citizens living in the European economic activity area, or does it apply to European citizens regardless of where they live?

Michele Neylon was the fastest on the buzzer. You have the floor, Michele.

MICHELE NEYLON: Thanks, Olivier. Giving a completely non-lawyer answer. The territorial scope is specified in article 3 of GDPR. My understanding/interpretation of it is that it applies to anybody in the European economic area. Whether they're a citizen or not is completely irrelevant. It also refers to where the data is being processed.

For example, if you were dealing with an American company who was processing the data within the EU, then GDPR would apply. If you're dealing with a European company who was processing the data

anywhere in the world, then GDPR would apply. I hope that helps to answer your question.

OLIVIER CRÉPIN-LEBLOND: Thanks very much for this, Michele. Indeed, quite a wider scope. Ricardo Holmquist is the next question. Pierre Bonis, you have put your hand up as well to this question. Pierre, do you have anything else to add?

PIERRE BONIS: Yeah. I [inaudible]. What is special about GDPR is that it changes the territoriality that was the basis of most of the rules of the EU to the customer location. It's not the location of the supplier. It's the location of the customer. So, of course we are talking about EU citizen, but if an EU citizen is asking for service while he's living in America, I think this is not applicable.

OLIVIER CRÉPIN-LEBLOND: [inaudible] the next question. That's from Ricardo Holmquist. I read this week that in Spain only 20% of the companies are prepared for GDPR. any clue if this regulation [inaudible]. Someone is using both the Adobe Connect and [inaudible]. They will need to mute. Thank you.

So, any clue if this regulation enforcement could be delayed? There is one, thing, though. The regulation has actually gone through. We're already in a moratorium time, aren't we? Thomas Rickert?

THOMAS RICKERT: Yeah. Thanks very much, Olivier. The [inaudible]. The Article 29 group, which is the group consisting of national data protection authorities, have stressed multiple times the independence of the supervisory authority. I guess there's no way to actually make them hold off with sanctioning. Although, the moratorium, at least in Germany, has not been unprecedented. At the time, when they safe harbor agreement was invalidated by the European court of justice, German DPAs have said we're not going to sanction before we get some more clarity on the succeeding agreement because it would leave everyone standing in the rain.

Yeah, I guess the situation is different and not different at the same time. It's different because GDPR is one-and-a-half years old. It's been out there. Everyone's had time to prepare. So, I guess in the ICANN world, we're facing particular challenges because we had letters from the Article 29 group dating back to 2003, which have been more or less ignored. So, I think expecting some grace period from them would likely not go down very well.

However, even the European Commission has asked for more time to discuss. They've asked ICANN to postpone the decision on a compliance model until after ICANN 61 in Puerto Rico. So, I think that that would probably be something that we could use to say we didn't get any clarity, and even the commissioner has asked for more time.

OLIVIER CRÉPIN-LEBLOND: Thanks for this, Thomas. Let's check of Athina Fragkouli is back online now and is able to speak to us. Testing one, two, three. Can we hear Athina? Unfortunately, we're not able. It's*6 I think to unmute.

ATHINA FRAGKOULI: Hello? Can you hear me now?

OLIVIER CRÉPIN-LEBLOND: Now we can hear you. Welcome back, Athina. The question that was fired over to you was if ICANN … Well, the whole thing about ICANN's existing WHOIS policy, although it is implicit by the absence of privacy policy that protects individual rights, if ICANN wishes to continue with this implicit policy based on RIPE's experience coming to understand the GDPR, what do you think that ICANN needs to do to legitimize?

ATHINA FRAGKOULI: Thank you very much for the question. I'm afraid I am not very familiar with ICANN's policy, so I cannot really comment on what ICANN does and how the process is set. But, I can give you some insight on the way [inaudible] national authority requests are dealt by the RIPE NCC.

Again, in article 3 of the RIPE [inaudible] terms and conditions, it's defined in the purposes in the RIPE database that the purpose of the RIPE database includes also providing information about the registrant [inaudible] number of resources when the resources are [inaudible] being used for unlawful activities to parties not authorized under the [inaudible] receive the information.

Also, another of the services of the RIPE database is providing information to parties involved in dispute over [inaudible] registrations to parties who are authorized and is allowed to receive that information.

So, if contact details and personal data are already published in RIPE database, then those that have the right to receive this information under the law can indeed use this information from the RIPE database as long as they're published. When it comes to non-public information, we do not provide unless we have a [Dutch] authority order.

I hope this explains a little bit the way we are dealing with such a situation. Thank you.

OLIVIER CRÉPIN-LEBLOND: Thanks very much for this, Athina. Indeed, it looks like RIPE has really given quite some thought onto this. Now, there was a follow-up question from Eve Edelson regarding ISOC HQ dealing with the databases of members. What about in the chapter level? I guess that somehow fits with the question of whether something as simple as a mailing list is subjected to GDPR.

So many of our own organizations – At-Large Structures and others, companies in fact – run often databases or just a mailing list to inform client or colleagues or members of all sorts of information. Are mailing lists, something as simple as a mailing list, subjected to the GDPR? Who wishes to answer this one? Pierre Bonis.

PIERRE BONIS: Yes. A mailing list is subjected to the GDPR, of course. But, this is something you can do from the beginning. You don't have to ask. Oh, I think they'll have to ask every time you are setting up a mailing list. You have to ask if the members agree to be opted in, as long as they are members when the association is putting a mailing list on.

At the end of the day, the compliance is just having a piece of text at the end saying if you want to unsubscribe to the mailing list, just let us know, which is something that ISOC does for years and years, and maybe for the beginning of the Internet because ISOC has invented the netiquette. I'm not sure it's going to change the way ISOC is doing with this mailing list. Just giving the opportunity for the people to opt-out and asking for the opt-in when they sign for the membership.

OLIVIER CRÉPIN-LEBLOND: Thanks, Pierre. Michele?

MICHELE NEYLON: I think some people seem to think that GDPR is brand new, a whole new concept. The reality is it isn't by any stretch of the imagination. As others have mentioned, it's based on pre-existing legislation. And at a practical level, when you're talking about mailing lists and e-mail and how you handle that and all that kind of thing, it's something that, if you were doing it right, it won't be an issue. I mean, does GDPR? Yes, of course it does. As long as you have permission from people and you respect that permission and handle e-mail in a fashion that is responsible and permission-based, then you won't have problems.

If, for example, I sign up to your mailing list to buy – I don't know – I'm interested in buying cleaning products and then you start sending me e-mail about coffee, then that's a problem. But, that's always been the way. If you want to make sure e-mails don't bounce, that's the way you look after your e-mail lists anyway.

But, to answer the question in short, yes. Thanks.

OLIVIER CRÉPIN-LEBLOND: Thanks very much for this, Michele. The next question that is listed in the chat is one from Javier Rua-Jovet from the ALAC. The question is to anybody. Does ICANN under its bylaw obligations to take notice of international law and/or human rights consider protection of end user's privacy a legal obligation binding upon itself? Does it have any pertinence on the GDPR, RDS, and WHOIS discussion? I think that Javier mentioned a bit further down that he wished Thomas to try and take a stab at this one.

THOMAS RICKERT: Yeah, I'm glad to do that. Hi, Javier. Looking forward to seeing you in Puerto Rico in a couple of weeks. Now, this is a tough one because the GAC, for example, has made explicit mentioning of ICANN's bylaws as a justification for making [inaudible] processing WHOIS data and making it available. Having WHOIS data is within [inaudible] mandate. It is [inaudible] hard-coded into ICANN's bylaws.

Now, the question is what legal status do these bylaws have? As I mentioned earlier, if it is the wish of international government to

[inaudible] ICANN where its performing a public function, then potentially this stipulation in the bylaws can be used as a [inaudible]. Specifically, that would require a law or some other act of equipping the private entity with a public function. So, we don't have that. Therefore, I'm a little bit cautious to just jump to the conclusion and say it's in the bylaws and international laws and the bylaws, and therefore we can do everything via the bylaws.

The issue is that we have this [e61.b] dealing with public interest, and then we have [inaudible].

OLIVIER CRÉPIN-LEBLOND: We appear to have lost—

THOMAS RICKERT: … Dealing with legitimate interest. The hurdles for E, processing of data in the public interest are higher than for the legitimate interest. If every public interest would constitute a legitimate interest at the same time, we wouldn't really need an E.

So, this might be a little construed, the GDPR, on whether we can make use of the bylaws. Either we are 6.1e or 6.1f. I hope that this [inaudible]. I'm happy to discuss more maybe on site in Puerto Rico.

OLIVIER CRÉPIN-LEBLOND: Thanks for this, Thomas. Unfortunately, we lost audio for five seconds. Maybe what might have been a crucial sentence. You were saying – where do we have it? Scrolling is difficult. You were saying that … I'm

just trying to see here. [inaudible] 6.1e dealing with public interest and then we lost audio. Just the last thing about the public interest.

THOMAS RICKERT: 6.1e is processing in the public interest. That would typically require a law or an official [vesting] of the controller with the public function. If the government thinks that ICANN is performing such public function, then potentially we could use the bylaws as a justification for dealing with data under 6.1e.

The issue is, however, that if 6.1e is not applicable, the only route we could take on this is 6.1f based on legitimate interest. This is something that you read in the government letters. So, they're basically speaking of public interest, public policy objectives, and public benefits as legitimate interest. But, if you could play those via 6.1f with the hurdles for 6.1f being far lower than for 6.1e, that's the question why you need 6.1e in the first place.

This is why I'm struggling systematically, looking at GDPR using 6.1e in the public interest for such purposes or using the bylaws, per se. But, I guess the governments who have [called] this out as a solution should be more precise in helping us understand what they really mean. And yes, it's complex stuff. I agree.

OLIVIER CRÉPIN-LEBLOND: [inaudible] live stream. This webinar is being live streamed as well. There's a question from [inaudible]. Two questions, actually. We can probably take them both at the same time. How should companies

approach GDPR from the management standpoint? How does the GDPR differ from existing data protection legislation? Who wishes to? Pierre Bonis.

PIERRE BONIS: Thank you. I would say a little bit like Michele said in his presentation. The change is not too much in terms of core business, but it's a very big change in our internal organizations. It means that we are dealing now with something that is closer to an ISO 27001 approach than to the previous one that was simple declaration that you are compliant.

It's a management system and I think that the difficulty for some businesses are the difficulty for the businesses that are not familiar with the management system and the implementation of the ISO or EFQM systems. It's going to be difficult because, at the end of the day, this is not true that we have to be 100% compliant in May, but it is true that we have to show that we are in a considerable improvement and that we manage this improvement and it implies a way of organizing things internally that is a bit difficult sometimes.

So, this is the main change, being able to follow the progress that you do and the risk assessment that you do on personal data, as before it was just you say what you do and if you are wrong, you may be punished. It's a huge difference, and for some SMEs, it's a huge challenge.

OLIVIER CRÉPIN-LEBLOND: Thanks for this, Pierre. Next is Thomas.

THOMAS RICKERT: Yeah. Just to add to Pierre, I think companies who are in Europe and who have taken data protection laws seriously, they are probably in good shape and there's not too much to do. Although you [inaudible] data protection or data security management system which was required before, so there's some work to be done, but it's relatively easy I should say [prepared] to, let's say, non-European operators who are processing data of European data subjects, because in certain cases, you have completely different approaches to data protection in their respective [home country].

If you look at the US versus Europe, this is really a clash of culture in terms of data protection. Therefore, we're doing a lot of work in the area. I'm a lawyer working in private practice and we see that we have to do a lot of explaining to convey the spirit of GDPR and how it differs from the [inaudible].

OLIVIER CRÉPIN-LEBLOND: We're losing Thomas again.

THOMAS RICKERT: Okay. I had finished in the meantime.

OLIVIER CRÉPIN-LEBLOND: The last 30 seconds of what you were saying, please.

THOMAS RICKERT: Okay. I apologize. I was saying that it's relatively easy for European operators that have previously been compliant with applicable data protection laws, but for companies outside Europe, you really have a clash of culture, and that is difficult to inject into the companies' common thinking that you have to take an entirely different approach to data protection laws.

I guess the most prominent example of that is the difference between the US system and the European system. For those, it's much harder.

OLIVIER CRÉPIN-LEBLOND: Thanks very much for this, Thomas. I'd like to thank just another few seconds to thank all of you. Thomas Rickert, Pierre Bonis, Michele Neylon, and Athina Fragkouli for providing us with this insight on practical implementation of GDPR.

There's an exciting discussion going on in the chat as well and [inaudible] to take us through the discussion that is going on, but unfortunately we have run out of time. We could've gone for another at least 30 minutes on this. Time has flown.

Don't leave quite now. There's still a real-time transcription survey. The box that you see in the middle of the screen is real-time transcription. This is just an add-on that is there on a test basis. It's been helpful for some people where you can't really hear too well or maybe when you have challenges when it comes down to English. Anyway, rather than me rambling, perhaps I should turn the call over to staff to ask the survey now.

EVIN ERDOGDU: Great. Thank you, Olivier. Everyone, I'll be changing the AC room into the evaluation mode. It should take a couple seconds to switch. You'll see on the right-hand side of your screen the first survey question for real-time transcription.

The first question is the RTT feature of the Adobe Connect room is part of a pilot. Please select one. There are four options. Very helpful, helpful, less relevant, or not helpful. I'll give everyone a couple moments to answer and then move on to the next question.

Okay, thank you, everyone. The second question is asking about you all. Please self-identify all categories that describe who you are. You can check multiple boxes. The first is a person with disabilities, second participant for whom English is a second language, third participant who does not speak English, fourth participant who has limited or low bandwidth, all of the above, or none of the above.

Okay, thank you, moving on to the third question. What benefit did you get from accessing the real-time transcription feature? Choose as many answers as necessary. Again, you can check multiple boxes. First is greater understanding of the topic, ability to understand the session more effectively, provided the correct spelling of technical terminology, able to more fully participate and engage with the presenter, or all of the above.

Fourth question. How accurate was the live RTT including participant names, terminology, etc.? On a scale of one to five, one being not accurate and five being extremely accurate.

How useful was the RTT for this call in general on a scale of one to five, one being not useful at all and five being extremely useful?

Second to last question. Where else do you think this should be required? This is a multiple choice selection as well. You can click multiple boxes. Working groups, taskforces, ad hoc groups, RALO calls, ALAC calls, CCWG calls, other constituencies, or all of the above.

The final is any final comments. This is a short answer if you have additional feedback or ideas or comments. Feel free to write here. Otherwise, we'll also be sending out this survey after the call to those invited to the call. So, you can fill out the survey manually on Google Forms. If not, just feel free to write in this box here and we'll try to capture your comment. Thank you.

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Evin, and thanks to everyone for having responded and answering these questions. Once again, thanks Thomas, Pierre, Michele, Athina. Great session. This is all recorded. It's going to be both on the live stream and also as a recording of the Adobe Connect on the relevant page and that will of course be stored for prosperity. You can come back to it in about 5, 10, 15, 20 years' time. Who knows?

In the meantime, it's 38 minutes past 20:00, so 20:38 UTC. We're a little late, as per usual, but it's been really super. So, thanks to everyone, and thanks of course to all the people who have not only asked questions but been present. At some point, we had 20 people on the livestream and 40-something – actually more than 40, nearly 50 people, 48 I think

– just participants in addition to our presenters and to the staff running the call. Very well attended. Thanks, everyone.

Now this session has ended. It's over. Have a very good evening, everybody. Good morning, good afternoon, and good evening and goodnight to those people that are in the right time zone. Take care, goodbye.

EVIN ERDOGDU: Thank you, all. This call is now adjourned. Please don't forget to disconnect your lines from the AC room and bridge. Thank you very much for your participation and have a wonderful rest of your day. Bye-bye.

[END OF TRANSCRIPTION]