GISELLA GRUBER: Good morning, good afternoon, and good evening to everyone. Welcome to the first webinar of the 2018 At-Large Capacity Building Program on the topic of data protection. What do you need to know as End Users about GDPR?

This webinar is held on Wednesday, the 24th of January of 2018 at 13:00 UTC. We will not be doing a roll call, since this is a webinar. However, we have French and Spanish interpretation. May I please remind everyone to state your names before speaking – and this is every time you do speak – to allow our interpreters to identify you on the other language channels, as well as for transcription purposes. Could I kindly remind all participants on the phone bridge, as well as on the Adobe Connect, to please mute your speakers and microphones when not speaking? A reminder to mute is *6 and to unmute is *7.

Last but not least, please do speak at a reasonable speed to allow for accurate interpretation.

Thank you all very much for joining and I will now turn it back to the chair of the At-Large Capacity Building Working Group. Over to you, Tijani.

TIJANI BEN JEMAA: Thank you very much, Gisella. Good morning, good afternoon, and good evening everyone. Today, we have in my point of view one of the most interesting webinars because the GDPR is a subject that all the ICANN

***Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.***

community – and all the Internet community, in fact – should be interested in, as it will impact the future of the [active] DNS WHOIS.

Even if we are not using a registrar or registry [inaudible] located in Europe, if it is not in Europe, even if it is not European enterprise, we can be subject to the compliance with the GDPR because this registry or registrar is serving the European [inaudible]. So, it is a very important subject from my point of view. It is especially important because we have a very tight time to be compliant with the GDPR. That's why there is [inaudible] work done and needs to be done in ICANN about this subject.

We have today two very important speakers. Thomas Rickert is one of the chairs of the CWG Accountability. We have to be very smart in doing this job. Of course, he has a lot of other hats, but I would like to [inaudible] on this one because he made a very good job and he is still making a very good job.

And Chuck, you know of Chuck because he's the chair of the working group about the next generation [inaudible]. Chuck, we invite the team [inaudible] and he gave us a very good presentation there, also.

So, I give the floor back to the staff for housekeeping announcements and then we'll come back to the presentation. Gisella, please.

GISELLA GRUBER: Thank you very much, Tijani. For those on the Adobe Connect, please see the housekeeping presentation displayed on the screen. For the others, I will be running through it now. For questions and answers during this webinar, you can see on the bottom left-hand side of the screen and these will be directed to the presenters.

Please do, however, note that we do have a question and answer presentations and pop quiz questions. Regarding the pop quiz questions, we will display these after the presentations on the side of the Adobe Connect room, so for all those again in the Adobe Connect room, please do be ready to join us in the session and to answer the questions by the polling tool.

Finally, at the end of the webinar, after the question and answer question, we will have a user experience survey composed of seven questions. We would very much appreciate if you could stay around for an extra three minutes or so to complete them. It is very important feedback for this At-Large Capacity Building Program that we are running.

Thank you very much, and back over to you, Tijani.

TIJANI BEN JEMAA: Thank you very much, Gisella. Our presentation, our two speakers, we have first Thomas Rickert to explain the GDPR and to give a general presentation of the GDPR. Then, he'll ask how [inaudible] the work of ICANN.

Then, Chuck will speak about the work that the working group is doing. First about WHOIS and RDS and then what they are doing now for the compliance with GDPR. So, Thomas, please go ahead.

THOMAS RICKERT: Thanks very much, Tijani. Thanks very much, Gisella, Heidi, and Silvia from staff for inviting me. I'd like to welcome all of you to this webinar on a very important and hopefully interesting subject. I would like to apologize up front to Camila and Sabrina, and to Jacques and Claire, the Spanish and French interpreters because they will probably have a very difficult time translating all this legalese into the respective languages.

I also have to say that I'm very happy that I can speak first, because speaking after Chuck Gomes whom all of you know and respect is going to be even a bigger challenge than speaking before him.

But, now, let's dive into this presentation without any further ado. You will see that I've brought a lot of slides. Don't be afraid. Many of them are graphics. Most of them are not very wordy. But, I wanted to provide you with a deck of slides that you can go back to and read a little bit in order to digest all the information more easily that you will be confronted with in the next 90 minutes.

Now, GDPR is a very broad topic, so please don't expect me to make all of you experts on GDPR in this limited amount of time, but I have agreed with Tijani up front that I would present some of the general concepts of the General Data Protection Regulation and then focus on some specifics for the domain industry that end users should understand because we're going to see probably some big changes in the domain industry taking place.

Also, there will be debates – likely, very heated debates – in the weeks and months to come. I'm sure that, as we go through this, you will understand better what these discussions are about and I guess you will be able to participate and join the discussion more informed after you've heard what Chuck and myself have to say.

Now, a quick word about [ECO-DE], an association that I'm representing today. ECO is an Internet industry association based in Germany. It has more than 1,000 members from more than 60 countries. Many of you will probably know the DE-CIX, which is the commercial Internet exchange run by ECO and that is the biggest CIX traffic-wise in the world. I'm responsible for one part of this association that deals with matters of the domain industry and we have more than 150 countries working in that space in our membership. I think that adding the domain names under management up, ECO's members manage more than 60% of the global domain names.

Now, GDPR, the General Data Protection Regulation, is not new. In fact, it's a concept that's been discussed for many, many years, but it was adopted and published almost two years back. But, there was a time span of two years until it would get into force, i.e. until it would be enforceable. So, all those were saying this is brand new. Actually, it is already applicable. It will only be enforced as of May 21, 2018.

Then, there is a myth which I think you should understand or which we should sort out. Those who are familiar with European law making will most likely have heard of directives and these directives need to be translated into national laws. And until this translation process into national laws by the national lawmakers has taken place, it would not be applicable in the various marketplaces throughout Europe.

This is not true for a regulation. A regulation is directly and immediately applicable to all member states and to all those who are governed by GDPR.

Now, the goals of GDPR are – I'm going to read this out to you because it's quite telling – is to regulate data protection in a uniform manner throughout the EU to give EU citizens better control over their personal data and regulate how controllers may use personal data.

On the other hand, the [inaudible] of free flow of personal data within the EU and to regulate the export of personal data outside the EU.

Now, if you just read that, there are a couple of takeaway messages for you. One, GDPR is about personal data. Data that is not personal data is not governed by this law. Then, the question is what is personal data? Personal data is basically data that allows for identifying individuals. So, according to our Supreme Court decisions, even IP addresses – even dynamic IP addresses – can be personal data because somebody will have log files to see who has that dynamic IP address at a specific point in time. So, it goes far beyond just the main address of an individual.

But, it's quite far-reaching. Domain names can be personal data if they allow for a data subject to be identified.

Then, certainly, e-mail address, phone number, physical address, fax number, all that would constitute personal data.

Then, this is for the EU. The sentences I read out for you also says that free flow of personal data within the EU shall be facilitated. That's relatively easy. But, whenever we're talking about the export of personal data outside the EU, things become more challenging. So, in future, if a registry or registrar wants to disclose data to somebody who's requesting that data, not only do we need to take a look at whether that disclosure in principle would be lawful, but we would also need to take a look at where that data is going, where the requestor is sitting and apply additional diligence in order to ensure that this export of personal data is legitimate.

Some of the main themes are increase transparency requirements. So, all those who are handling personal data need to properly document what they're doing. They need to be able to inform data subjects as well as data protection authorities about what they're doing with the personal data. So, there needs to be process documentation, which we call the record of processing activities. And they need to be able to prove, for example, that they got consent by the data subject where consent is part of the system that is used to obtain personal data.

Then, there are increased data security requirements. There are increased accountability requirements. I guess the most important one there is a reporting duty in case there are data breaches. Data breaches can come from the outside, intrusion. Data [inaudible] be disclosed is widely shared or handed over to third-party. There can be a breach manipulation of data. Changes to the integrity or correctness of the data can be a data breach and those breaches can be from without as well as from within. It may well be that an unfortunate employee makes a mistake, data is corrupted, and then the question is: what happens? Then you need to carefully assess whether you need to inform the supervisory authority of that breach and whether the data subject's concern need to be informed as well.

There are strict timelines that need to be abided by. You need to fix thing quickly. We can see from that, that the lawmakers are taking this very seriously and they want to ensure that nobody is able to hide or keep secrets when there are substantial data breaches.

Then, what's new is the right to be forgotten. So, if you're a customer of a company and you don't want to be with that company anymore or with that social media platform, you have a right to be forgotten. But, that only goes as far as the other duties for an operator to keep that data let's say for bookkeeping requirements or fulfilling bookkeeping requirements or other legal requirements.

Then, there is the right to data portability. So, if you are with Company A today and you want to change your operator and move to Company B, then there must be a possibility to take the data with you.

Then, two more concepts that I want to outline very briefly are privacy by default and privacy by design. Privacy by default means that the settings in a software environment need to be very strict to start with, so that basically the customer goes to a social media platform, just to stick to that example, and they can then loosen the requirements and show more data publicly. But, the basic setting must be restrictive and it must be user controlled to make it less restrictive.

Privacy by design means that you have to design your IT systems in a session that they don't collect and store more personal data than required. So, you need to make sure that even if you are hiring outsource software developers that you make sure that they program their stuff in a fashion that is actually following the principle of data minimization.

Let's now look at some principles for lawful data processing. This is going to be decisive for the rest of our conversation. That's enshrined in Article 6 of the GDPR. Processing shall be lawful only if and to the extent that at least one of the principles is applicable.

That would be consent. You can either ask the data subject for consent. We'll talk about consent in a moment in a little bit more detail. Then, you are entitled to process data to perform a contract. Then, there is lawful processing to fulfill a legal obligation. So, if there is a legal obligation for me as a registry or registrar to process data in a certain way, then I don't need, for example, explicit consent for the data subject, but I can just do that because [inaudible] legal obligation for me.

Then, the data processing that is necessary in order to protect the vital interests of the data subject or of another [neutral] person. Data processing in the public interest or in the exercise of an official authority vested in the controller. That's for public authorities.

This is going to be another important clause. Legitimate interest pursued by the controller or by a third-party, except where such interest are overridden by the interest of fundamental rights and freedoms of the data subject, which require protection of personal data. In particular, where the data subject is a child.

Now, what does this mean in practice? Let's bear in mind that for at least the first part of our conversation, A, B, and F will be the most important ones. A was consent based processing. B was processing to perform a contract. F was processing based on a legitimate interest.

Now, if you're wondering what performing of a contract means, basically it says if you are an online bookshop, then you don't need additional permission from the customer to ask the customer for the shipping address for the book. They need to know the address where the book can be shipped to physically because otherwise they wouldn't be able to fulfill the contract with the customer. That's behind it.

There's a lot of confusion around that specific clause and this is why I'm highlighting it now because it is always the contractual relationship between the data subject, i.e., the customer, and the operator. In the domain name world, we would need to look at the contractual relationship between the registrar or the reseller and the registrant.

There are many folks who think that the registrars obligations vis-à-vis ICANN – that contract, the Registrar Accreditation Agreement – could be used to legitimately process data to perform a contract. But, that's the wrong contractual relationship.  So, please keep that in mind. I'm sure you will hear more talk about that in the near future.

Let's look at consent for the moment. Consent is what currently in the domain name system for generic top-level domain names what processing is based on. So, in the Registrar Accreditation Agreement it says that the registrar must obtain valid consent from the data subject. But, there's an issue with it because the controller must be able to demonstrate that the data subject has consented. That might be possible. But, then, the data subject can always, without giving any reason, withdraw the consent that was given. So, if you base your data processing on consent and then the data subject withdraws the consent, you're in trouble.

Then, the content must be given freely. There's a prohibition of coupling. What's happened so far in the domain industry is that the registrars or the resellers told the customer, "Yes, you can have that generic domain name, but you can only have it if you agree, if you consent, to your data being publicized via WHOIS." That, according to the legal assessment that ICANN asked from the Hamilton Law Firm as well as based on information that we got from the Article 29 group, which is a group where all the national data protection officers of the European member states convened, they said that is an infringement of the prohibition of coupling.

So, consent is problematic or it can be problematic in a complex system such as the generic domain name administration.

Then, to whom is GDPR applicable? You might say I'm outside the EU, so I'm fine. I don't have to care. Probably you will have to care because GDPR is applicable not only to data controllers and data processors inside the EU, but also to those who are handling personal data of data subjects in the EU.

So, if you are serving EU citizens, even though you might be outside the EU, and if that doesn't only happen occasionally, GDPR will be applicable. In that case, you have to appoint a representative inside the EU. The representative is there to respond to information requests from data subjects, but also for communicating with the authorities.

Now, sanctions. There's been a lot of talk about GDPR and sanctions. In fact, many of the principles you find in GDPR are not new. There are some strict data protection regimes in Europe where most of the [IDS] have been applicable for many, many years. But, there was a deficit of sanctioning. So, the supervisory authorities didn't really go after the companies that were not in full compliance with applicable data protection laws.

Now, under the GDPR, this is going to change because we are going to see fines for minor issues up to 10 million Euros or 2% of the global annual turnover. For severe infringements or breaches of the GDPR, it's up to 4% of the global annual turnover or up to 20 million Euros. That certainly has a deterring effect on those who are working with personal data.

Then, there's another issue because aggrieved data subjects that report to the authorities can take the authorities to court in case the authorities don't take action. So, user groups do have the power now to force the authorities to take their report seriously and analyze them and take action where needed.

Now, what does this mean for ICANN and the generic TLD world? Now, there have been a lot of discussions with ICANN and ICANN certainly is in a predicament because the WHOIS topic has been discussed for ages. Fadi Chehadé whom all of you remember as ICANN CEO, when he did his inaugural speech at an ICANN meeting, he said there seemed to be two issues in the world that obviously can't be resolved. That's the Palestinian conflict and WHOIS. I'm not sure whether I would have chosen this example, but it certainly shows the complexity of the WHOIS debate, where on the one end of the spectrum you have those who have a great interest in having all that data publicly available. That's the security industry. That's IP lawyers. That is law enforcement. That might also be individuals that just want to know whom they're doing business with online.

Then, on the other end of the spectrum you have those who are interested in data protection. These positions were hardly reconcilable. So, therefore, ICANN had obviously an issue with just talking to the registries and the registrars and deal with this as a matter of contractual compliance, but this, according to my humble view, is actually the top priority.

Under this new regime, the data controllers and the data processors – and we'll talk about those concepts a little bit more later during this presentation – they are facing the risk of being fined. The IP lawyers, the Internet service providers, the businesses that are just using the DNS, they are not running the risk of being fined. I think, therefore, ICANN needs to make sure that as a matter of priority, compliance is established between ICANN and the contracted parties.

So, what ICANN did in Abu Dhabi, what [inaudible] did in Abu Dhabi, he announced that ICANN will be dealing with this in two phases. First of which will be the contractual compliance phase for the interim, so that companies that don't follow the letter of the registry and registrar agreements or registry agreement and registrar accreditation agreement don't run the risk of getting breach notices from ICANN.

In the longer term, there would be a community process because a lot of consensus policies and other bottom-up multi-stakeholder model based models need to be revisited for full compliance.

Now, what ICANN has done in the last couple of days, they have published three models and asked the community to comment on those models before January by January 29th. We can discuss these models a little bit more as we move on. I'm pretty much involved in all these topics not because I'm a lawyer working in this space, but also since ECO has developed a proposal, which we've submitted as a model to ICANN to be reviewed and that could be used as a compliance model, at least for this interim phase.

I'm now going to use some of the material that we used for presenting this model. Some of the ideas in there will not be universally accepted because some of them are controversial, but I think it will be valuable in understanding the complexity of the issue and the sore spots that we find in this industry.

Now, the models proposed by ICANN, they say let's focus pretty much of the disclosure of data. Everyone is talking about WHOIS when it comes to GDPR. But, in fact, you need to take a look at the whole process of collecting data as well.

As I mentioned earlier about the principles for legitimately dealing with personal data, you need to apply or you need to establish a legal basis for every single step of the processing from collection to changing data to transferring data to third-party, to deletion of data, up to disclosure of data publicly or semi-publicly via the WHOIS. The models proposed by ICANN only look at the disclosure part.

Also, ICANN is assuming that all models would collect all the data elements that are currently being collected and that is problematic because, according to the principle of data minimization, which I mentioned earlier, you need to take a close loo at whether you need all the data that currently is to be collected according to ICANN's contractual requirements and policies.

Then, it also assumes that our models and all models that data can easily travel from a registrar to the registry and that's at least something that also needs to be taken a closer look at.

Now, let's take a look at what parties are involved in processing of data in the gTLD system. What you find at the left-hand side of the visualization is the Internet user. So, the Internet user either goes through the reseller and inputs data with the reseller, or they go to an accredited registrar, and where the registrar has a reseller relationship, there's an agreement between the reseller and the registrar. Then, the registrar has a registry/registrar agreement with the registries and both of them have their respective escrow agents where data is transferred to.

Then, we have the [bureau] at the right-hand upper side of the slide, which is the emergency backend operator that kicks in whenever a registry failed. So, in case of registry failure, ICANN can request the data from the registry to be passed on either to ICANN and then passed onto the [bureau] or from the registry. I think there are two ways to getting that done. But, the [bureau] is also in the mix as well as the escrow agents for both parties.

Then, ICANN has contractual relationships with the registries and registrars and with the [bureau], so they are also party to all of this, not just an outside observer.

And we have WHOIS customers who want to get access to data at the registry or registrar level.

So, basically, what we tried to do is come up with a model that takes a look at the legal risks involved with data processing. So, you will remember that e had at the most relevant legal provisions 61a GDPR consent based processing, 61b which is processing to perform a contract, and 61f which is processing based on a legitimate interest claimed by the data controller.

You can allocate risk levels to those. The lowest risk is data that you process to perform a contract. That's what you need. You need to be able to link a domain name to a registrant, so that you can evidence that the registrant is actually the owner of a domain name.

Then, the medium risk level would be based on legitimate interest. So, if you say I want to process the data, I want to analyze all the data in my registrant base to find out whether there are patterns of illegal behavior, I want to do that for security reasons, then you can claim that as a legitimate interest, but in that case, there's a possibility for the data subject, for the customer, to say, "Well, my rights outweigh your legitimate interest, so I don't want to do that."

But, what you then do is a balancing of the legitimate interest against the interest of the data subject. If you have good reasons to process the data, then you might be able to continue to do so, but the risk is that the user objects. The highest risk is with consent-based processing because whenever consent is required, there is the risk that the customer just withdraws his or her consent and then you are in problems because you can't process the data anymore.

Currently, the data collected can be [inaudible] into various boxes. We have the registrant data, [inaudible] data, [inaudible] data, billing [inaudible] data, and then you have some technical data on registries and registrars. You have data about who the registrar and registry is. Then data that needs to be process based on a so-called data retention specification. And most of the registrars set up an account, so they actually also collect account holder data.

We think one needs to make a distinction between different registry scenarios. So, where the registry does not have any specific requirements, the equivalent to that would be dot-com, which is an open, generic domain name, so they might not need all the registrant data in order to give a domain name registration.

But, where there are nexus requirements that somebody needs to be a bank to get a dot-bank domain name, there the registry has an interest in actually doing a validation whether the registrant is an eligible registrant. And based on that, the registry can either request data to perform a contract – so, dot-bank we think can request all the data from the registrar because they need to be able to validate the customers. And where there are no such requirements, say it is possible to get that data from the registrar if there is a legitimate interest that can be claimed by the registry.

Now, let's move a little bit quicker now. The question is what actually is needed to perform the contract. We do think that the red boxes, the [inaudible] are no further required if you follow the principle of data minimization. You need the registrant data, but you don't need the rest, because in the case of technical issues, you can still talk to the registrant and most registrars would go to the account holder and not right to the tech [see] that is mentioned in WHOIS. The registrars would send the invoice to the account holder and they would not look at the billing contacts in the WHOIS.

So, according to the principle of data minimization, the basic setup would be the registrar collects the data of the registrant and then we would have some more technical data that is collected and only the domain name and not any further data apart from technical data is then transferred to the registry. And where the registry has special requirements or where the registry claims special interest, they can say so and then that data can be collected and pass onto the registry, but it needs to be specified in the registry-registrar accreditation agreement and we think that ICANN should not force people to do consent-based processing because that's the most vulnerable and most risky place.

In terms of who is responsible for all this, we have the registrars, the registries, and ICANN who according to our view as well as the Hamilton Law Firm, seem to be joint controllers. There are different scenarios for the other services such as [bureau] or escrow, but I'm not going to go into that detail now. This is just to show to you that it is important for ICANN, registries, and registrars to talk to each other because hen you service a customer, according to the new laws and the information and transparency requirements, you need to be able to tell the customer exactly who does what – i.e., the roles and responsible of the parties involved. And therefore, the responsibilities need to be sorted out very clearly.

So, I spoke about the basic setup. Can the registrar add additional data elements? Yes, they can, if they want to. But then they need to be responsible for that.

Can the registry add additional data elements? Yes, they can. But, only the basic data set to perform the contract should be enforced by ICANN. That could be nexus requirements, eligibility requirements, or even if the registry chooses to have a local admin [see]. Then the admin [see] data can be collected, which otherwise wouldn't be necessary to perform the contract.

Now, let's move on to the disclosure part. That, again, is a very difficult subject because all the data that you can lawfully collect you can't automatically disclose, and therefore you need to take a very nuanced look at what data can be disclosed.

One thing is for sure. As of May 25th, information can't be publicized as it is publicized today because you don't find a legal basis for that broad publication of data. This has been said by multiple legal examinations as well as by the Article 29 group.

So, what we think is we should basically set up a firewall and have a gated WHOIS process, where you can get access to the next level if you are a certified requestor. And law enforcement, at least in the EU could be a certified requestor because we can take for granted that they would only use this service for data lookups that are based in law, and there could be other certified requestors such as IP lawyers and others.

Privacy and proxy services can still be used because if somebody is a certified requestor and if you have an interest in your data being further protected, then they would only get access to the privacy and proxy service data at that level.

Now, then there are certain disclosures that we think can be based on performance of the contract because all the users are accepting UDRP and URS, so if you want to check whether you should use one of these policies to challenge a domain name registration or its use, then you need to be able to verify whether the registrant is a legitimate trademark owner and you can only do that if you get access to that data. So, that would be covered to allow for data access for these cases.

Then, for 61c, compliance with a legal obligation, if you have to respond to law enforcement data request, you have to follow them. But, this can only be used for disclosures to European law enforcement, as I mentioned earlier.

This visualization shows how the system could work, so you would have European law enforcement that has another directive based on which they can request data and non-European law enforcement would need to go through mutual assistance agreements in order to get access to that data.

That is certainly disastrous for law enforcement at the global level, and therefore we think the lawmakers need to make sure that appropriate legal tools are available to make data access easier for law enforcement. But, in the absence of those tools – and I should add in brackets that the lawmakers I think have forgotten to put something like that in place because they thought WHOIS would be open forever. In the absence of that, it is not acceptable that the registries and registrars take the risk of unlawful processing. So, we are in favor of a gated access.

I think I should stop here. I mentioned to you that WHOIS would be more or less closed.  You would still get the opportunity to write to the registrar, to pass on messages to the registrant in case you have something that you want to communicate with them, but you don't get access to the data for that purpose. Then we have the certification program where certified requestors can get access to the second tier of WHOIS. Others would need to file individual requests or send subpoenas that would need to be analyzed. And in order to facilitate the whole process, we're proposing that a centralized clearinghouse could be set up to manage those disclosure requests.

All this could be easily or more easily done based on the WHOIS protocol successor RDAP, where you can have those certification authorities and different access rights for different parties.

So, I guess, with that, this is all for your reading pleasure when you get the slides. Take a look at that. I mentioned the gist of that, and in the essence of time, I'm going to stop here and thank you for your attention.

TIJANI BEN JEMAA: Thank you very much, Thomas. Thank you for this very good presentation. I know that time is not enough to present GDPR. But, we need to go to Chuck [inaudible] who will tell us about the work they are doing in the working group and especially the work they are doing to reach the compliance with GDPR. Chuck?

CHUCK GOMES: Thank you very much, Tijani. Thank you for the invitation and I appreciate the opportunity to briefly go over the relationship of the Next Generation Directory Services PDP to replace WHOIS. I will be relatively brief because I am not a GDPR expert. I want to compliment Thomas for a great presentation. He put an awful lot of information together in a very brief period of time, so my compliments, Thomas, on that.

Going to slide two – and notice I only have seven slides here – the basic thing I want to focus on is what is the relationship of the GDPR to the RDS policy development process. In doing that, I'll very briefly talk about the goal of the PDP, give you a brief idea of our current status, and then talk about how the PDP relates to the GDPR.

Going to slide three, summarized here is the goal of the PDP Working Group. We are tasked with defining the purpose of collecting, maintaining and providing access to gTLD registration and data, and considering safeguards for protecting that data, including of course protecting according the GDPR, and in the case of Europe and dealing with [inaudible] in Europe.

Our charter – and I think most of you know the GNSO provides a charter for every working group, and in particular PDP working groups. I'd like to note that there are three phases to our work, as you can see in the middle left there.

The first phase, which we are still in, is defining requirements for any RDS system to replace WHOIS. Once we get the requirements defined, and there are certain processes that have to take place and approvals before we get there, we would then develop policy to meet those requirements in phase two. Then, in phase three, develop implementation guidance. Of course there are pre and post steps to all of these things.

One of the key things to understand, there’s a fundamental question and I’m focusing on the little paragraph middle right there where it says “tasks to be completed” and it says, “If and why a next generation RDS is needed.” That’s a fundamental question that the working group needs to answer. Is a new RDS system needed or could the existing system be modified to meet the requirements that we developed especially in the first five questions out of eleven in phase one? We’re still in that area.

If you look at the flow charts there, I already pointed out that we’re still in phase one. In fact, in the earlier part of phase one, but probably the more difficult part of phase one. If, in fact, the working group recommends that a new RDS system is needed and we complete all the requirements for phase one, only then would we go to phase two for development of policy and then phase three, implementation.

Let's go then to slide four. During phase one, what we're trying to do in the working group is to attempt to reach consensus on the following questions. I already talked about the fundamental requirements, but the charters for each of the phases involve eleven questions or eleven categories of work.

Before we answer the question of the fundamental requirements, whether a new system is needed, we're supposed to at a minimum consider users and purposes and associated access for registration data, accuracy of data, what data element and privacy requirements. Obviously, Thomas has done a very good job going through the privacy requirements related to the GDPR. Of course, there are many other jurisdictions around the world that also have specific privacy requirements.

There you see on the third bullet on slide four that fundamental question. Is a new policy framework and next generation RDS needed to address these requirements? If yes, then we will need to develop requirements related to six other areas, coexistence of the new system with the current system, compliance, a system model, cost-benefit and risk analysis requirement. So, we're not there yet. But, that, as you'll see on this data slide.

If we decide that a new system is not needed – and I'll qualify that by saying I think most of us realize that seems very unlikely, but we still have to answer that according to our charter. But, if the answer was no, we would have to show that the current system can be modified to meet the requirements.

Going to slide five, you can see the timeline. The board resolution was made in April of 2015, charter approval happened in November of that year, and then two years ago this month we started the working group. So, we had been working two years. We're starting out third year right now.

In June 2016, we developed a possible requirements list. In November of 2016, the deliberation began. It really didn't end on the specific requirements. Our target right now is by June of this year to start developing our first initial report. Now, for those familiar with the GNSO processes, there's usually only one initial report. Just for phase one, we are planning to do two initial reports, so that we can get some significant feedback from the community, including the At-Large, at that point. That would come after we have dealt with the first five questions in our charter.

So, the next steps. We need to finish deliberating on charter questions one through five and answer that foundational question of whether a new system is needed. We would develop the first initial report, and like I'm showing on the balloons there, the last balloon shows we're hoping by June of this year to start preparing that first initial report for feedback from the whole community.

Now, let me just qualify right there. Feedback into the working group is welcomed throughout the process. The At-Large has a variety of its members who are participating in the working group and input from the At-Large of course is welcome and individuals is welcome throughout our processes.

So, after we get the results of the feedback from that first initial report, we would modify our work plan as needed and then, assuming that we say that a new system is needed, we would deliberate on the remaining charter questions – questions six through eleven. And then produce a second initial report and a final report that the GNSO Council would receive and then, assuming approval from the Council, move on to phases two and three.

Now, the charter envisions that phases two and three might be able to be done concurrently, but that's a decision that is a ways off at this point.

Going to slide six, and my next to last slide. The key question I think for this session today is how does the GDPR relate to this PDP? First of all, let me say, as the first bullet says, that this is a bottom-up multi-stakeholder process and it's going to take multiple years, like everything has with WHOIS over the last 17 years.

The PDP must address global data protection requirements, not just those from Europe. It so happens, though, that the GDPR provides an excellent example of data protection and privacy requirements for handling natural persons personal information.

So, we're, as a working group, focusing very closely on what's happening with GDPR because it does serve as a great example for us of data protection requirements.

The work now being done on GDPR compliance for today's WHOIS that ICANN is involved in, that registries and registrars, that ECO is involved in and Thomas is very active in, will be used by the PDP as applicable. We're hoping that all of that work will save us some time going forward.

It's really important – and I'm on the fifth bullet right now, the next to last bullet. Any next generation RDS would be a long-term solution for handling privacy and data protection requirements. The only way to change registration data requirements and registry and registrar agreements is through a PDP, except if ICANN were to implement emergency policy changes and both registry and registrar agreements do allow for that.

So, in the short-term work that's going on to help deal with the fines that Thomas mentioned going into effect May 25th, that's very important. It's needed. But, it is not policy development. So, it's very important to understand that.

Any such emergency policy changes will not predetermine the recommendations of the PDP Working Group, unless the working group itself supports those changes through the bottom-up policy development process.

Then, my last slide – slide seven – is just to thank you. Of course, we're going to have a Q&A and there will be some pop quiz questions and so forth. I welcome the opportunity to respond to your questions. Thank you.

TIJANI BEN JEMAA: Thank you very much. Thank you, Chuck. Thank you very much for your presentation. Before giving the floor to the staff for the pop quiz questions, I would like to ask you, Chuck, please explain the difference between the thin and thick WHOIS. As you know, the [EU] has proposed [inaudible] and he is speaking about [inaudible]. So, it is a way to make our community understand the model that he is speaking about, first by understanding the difference between thin and thick WHOIS. Can you please?

CHUCK GOMES: Sure. Thanks, Tijani. Most of you know that one of the successful GNSO PDPs relating to WHOIS relates to thick WHOIS. That was accepted as approved as a consensus policy, first by the GNSO Council and then ultimately what really counts is by the ICANN board. That particular consensus policy is in the implementation phase, but that phase has been delayed because of data protection and privacy requirements like the GDPR.

In trying to implement thick WHOIS at the registries that are still thin, everyone began to realize very quickly we've got a problem of transferring all this thick data to registries.

So, that has been solved through the [inaudible] of people who were looking forward to that happening. But, there are some real serious problems. What Thomas just shared with all of us I think most of you can probably see the problems if all this thick data was all of a sudden transferred to registries by registrars. So, that’s a problem that hasn’t been solved.

I’m going to share a personal opinion in that regard. I think probably, because the PDP recommendations of the working group for thick WHOIS have already been approved, I think probably those particular recommendations are going to have to be sent back to the working group – or at least that’s one option – so that they can be looked at again in light of things like the GDPR. So, that’s a very good question, Tijani, for this webinar.

I made the assumption that everyone understands the difference between thick and thin WHOIS. If that’s not the case, please let me know because it’s a very important distinction.

Now, in the working group we have stopped using the term thin WHOIS and we’re using a term called the minimum public data set and we’ve reached rough consensus agreement so far on certain elements that are a part of that minimum public data set. Like Thomas pointed out, that’s very much reduced from what we’re used to today in WHOIS.

If I didn’t answer your question satisfactorily, Tijani, please let me know.

TIJANI BEN JEMAA: Thank you very much, Chuck. Now that people know that thin means a minimum of data. The thick WHOIS is the whole data that you give to the registrar when you buy a domain name. The thin WHOIS is the minimum information to be public. That is the difference between the two, thin and thick.

Thank you very much, Chuck.

CHUCK GOMES: Tijani, just to add one minute of comment on that. I think most people know this, but dot-com and dot-jobs are thin registries, so to speak. They only offer a minimum amount of WHOIS data. You have to go to the registrars to get the thick data. That, hopefully, ties it together a little bit.

TIJANI BEN JEMAA: Thank you very much. Before going to your questions, first we will go to the pop quiz questions. Gisella, please, can you go ahead?

YESIM NAZLAR: Hello, Tijani. Before we move onto the pop quiz questions, I see there are a couple of questions in the question and answer [pod] from Alfredo Calderon to chat. Would you like me to read them out now or would you like to cover those questions after the pop quiz?

TIJANI BEN JEMAA: We will start with them when we reach the Q&A part. Now we are in the pop quiz questions.

YESIM NAZLAR: Okay, perfect. Our first pop quiz question is: Is it appropriate for the ICANN organization to be working with the community to try to develop an approach for complying with the GDPR by May 2018? Is yes or is it no? Please [inaudible] now.

CHUCK GOMES: Are these questions for Thomas and I, or are they for the participants in the webinar?

TIJANI BEN JEMAA: No, they are for the participants. They are the questions that you gave before the—

CHUCK GOMES: Okay, that's what I thought. I just wanted to be clear.

YESIM NAZLAR: Yes. Chuck, I would like to learn the correct answer from you, please.

CHUCK GOMES: Thomas, please feel free to jump in on this, too, because you're very actively involved in even leading a lot of this work that's going on right now to prepare for the May 25th target date.

I think the answer is yes. It is appropriate. In fact, it's necessary because current contractual requirements for registries and registrars conflict with regulations like the GDPR. So, something has to be done or there's a serious problem, especially or contracted parties. I think it has to be done.

But, the important distinction is that should not be considered as policy development. There may has to be some emergency policies put in place by the board to deal with this conflict. But, it's just important to make the distinction that that's not policy development. The GNSO has very well-defined processes for developing policy, and only when those processes [that are followed] can long-term changes to registry and registrar agreements be implemented.

So, a short-term fix or fixes are needed, so it's appropriate that ICANN, the community, and the contracted parties be working on this, but at the same time, we must recognize that doesn't replace the policy development process that's going on.

Unfortunately, policy development, because it's multi-stakeholder and bottom-up, is very slow. So, there's no way that the policy development process can happen in the short timeframe we have in front of us.

TIJANI BEN JEMAA: Yes, Chuck. It will not replace it, but for the question, it is not only appropriate, it is necessary in my point of view. Can we go to question number two?

YESIM NAZLAR: Of course. Moving on to the second question. Our second question is: will the work of the Next Gen RDS PDP Working Group be necessary if ICANN is successful in its current support to develop an approach for complying – sorry, [inaudible] same question. Apologies, it's my mistake.

TIJANI BEN JEMAA: Okay. Yesim, before continuing, please I would like to give the floor to Thomas who is raising his hand. Thomas, is this about the question?

THOMAS RICKERT: Yes. Thanks very much, Tijani. I'd like to take the opportunity to respond to the first question as well. While Chuck is correct in saying that this needs to be discussed with the community, and that is not policy development, I think we need to be crystal clear that GDPR requirement as well as requirements stemming from other national or regional data protection laws need to be complied with. That is nothing for the community to shape.

Basically, the bare minimum of what needs to be done so that the registries and registrars and ICANN are not facing the risk of being sanctioned is a matter of compliance, and while the community needs to be informed about what's going on, this is something that I think needs to be done primarily between the registries, registrars, and ICANN.

Nonetheless, the community process needs to be done either subsequently or in parallel because what gives legitimacy to all the things that registries, registrars, and ICANN are doing is the bottom-up multi-stakeholder process and the shaping of consensus policies. And these consensus policies have the beauty that they are immediately applicable to all registries and registrars without the need to formally change the contracts for the registries and registrars.

So, in order for having a long-term data protection related solution, we need consensus policies as a solid foundation for the operations of this whole industry. But, these consensus policies must not go below the minimum of what's required to be compliant.

At the same time, just to give you an example, if the community says we want WHOIS to be publicly available as it is today, then that might be the community process, but it wouldn't be compliant. Therefore, we need to do the contractual compliance part first to establish what needs to be done in order to avoid sanctions. So, that is the [must]. Then the way how we do things or what we might be doing on top of it, that is subject to community consensus and ICANN's bottom-up policy development process.

TIJANI BEN JEMAA: Thank you very much for this [inaudible]. Yesim?

YESIM NAZLAR: Moving on to question number two. Will the work of the Next Gen RDS PDP Working Group be [inaudible] if ICANN is successful in its current support to develop an approach for complying with the GDPR by May 2018? Is it yes or is it no?

CHUCK GOMES: The answer is yes. I think I basically explained that already. The policy development process has to happen if you want long-term changes to happen in the registry and registrar agreements related to RDS data. Any emergency policy that would be put into place to deal with the issues that Thomas made very clear, those are only temporary. Ultimately, we will have to have it implemented with appropriate changes to deal with all the requirements of GDPR and other regulations from dozons of other jurisdiction around the world to happen in the long term. So, the answer is yes.

YESIM NAZLAR: Thank you, Chuck. I'm now moving onto our third question. Which of the following statements is true? A, I may publish personal data that I locally collected; B, local collection does not mean that I may publish personal data. Please cast your votes now. Maybe Thomas can give us the correct answer for discussion.

THOMAS RICKERT: Thanks very much. Answer B is the correct answer. As I mentioned during my presentation, you need to find a legal basis for every step of processing personal data. The mere fact that you have legitimately collected data does not mean that you may publish it in the WHOIS directory.

YESIM NAZAR: Thank you very much, Thomas. I'm now moving on to the final question. My company is based in Australia and I only serve customers from Australia to New Zealand. Is GDPR applicable to me? Is it yes or is it no? Please cast your vote now. I would like to [inaudible] Thomas as well.

THOMAS RICKERT: Yeah. Thanks very much. The basic principle is that if you are based outside Europe, which is true for Australia, and if you are not serving data subjects in the EU, which would be true in this example, because this company is only serving customers from Australia and New Zealand. In that case, GDPR would not be applicable. Answer two would be correct.

YESIM NAZLAR: Thank you very much. This was the end of our pop quiz section. Back to you, Tijani.

TIJANI BEN JEMAA: Thank you very much, Yesim, and thank you Chuck and Thomas. Now the floor is yours. You have questions for them? I will start by making a comment. Yes, the GDPR is wonderful [inaudible] regulation. But, for the application of this regulation, I see several concerns, if you want. When you speak about content, you know any service you ask for you are asked to consent that they collect your data, so you are not free to give or not give. If you want to have the service, you have to give the data. The content is more or less [automatic].

Second point in the GDPR. Those who hold the data are obliged to erase it as soon as the use of this data for the purpose for which they were collected is finished. How do you be sure? How can you control that? How can you [inaudible] that? It's very complicated. I don't know the implementation of this regulation would be so difficult.

THOMAS RICKERT: Tijani, before I answer, can you repeat the second question for me, please?

TIJANI BEN JEMAA: Yes. Those who collect the data, they have to erase the data. They have to destroy the data as soon as they have finished to use it for the purpose for which they are collected. But, how do control that? How to monitor that? How to know if it is done or not?

THOMAS RICKERT: Thanks very much for these questions. With respect to the first question, it is true that when you subscribe to services, you're often asked for your consent. There are scenarios where, let's say, a service is offered for free and where you basically have a deal with the operator that you give the data in order to obtain the service. So, if that model is changed, then basically this free service, to use that example, couldn't be offered anymore. So, there's a direct relationship there with the data provision with the service.

In those cases, it may be okay to ask for the consent without violating the prohibition of coupling. In the case of domain name registrations, this is somewhat different because you are paying for the domain name and the publication of data via the public WHOIS system is not inevitably required to make the domain name registration possible. And there are examples in the ccTLD world today where you register a domain name, but your data is not being disclosed.

So, we do not think that it is easily possible. We rather think it is hardly possible or it is very high risk to create a system that is consent based for publishing WHOIS data.

But, it may well be that you have certain registrant groups that are gladly providing their consent and where the registry comes up with the consent-based model for WHOIS.

This is not authorized by the operators of dot-bank or dot-insurance or equivalent, but I could envisage a scenario where the registry for such a high-trust TLD says, "Okay, we see that our registrant base has a huge interest in the data being publicized," because they want to make it easy for customers to check that they're actually dealing with a real bank or with a real insurance provider.

The second question with respect to retention period is a good one. There are different retention periods for different types of data. So, it becomes even more complex when it comes to retention periods that meets the eye, because the bookkeeping requirement, so the tax authorities can come in and expect your records, you might have very long retention periods, while just for the provision of the service, you might not have a very long retention period.

So, if you look at all the data that you're processing, it is very well possible that you have different retention periods for different data elements. How would you control that? Every company that falls under the GDPR needs to have a list of processing activities and they also need a data protection management system. This system, which is basically a repository of different policies to deal with data needs to specify the retention periods for the various data elements as well.

If the authorities are knocking at your door, you need to be able to proceed those policies to them and explain to them exactly what you are doing in order to ensure that data is erased when it is erased. So, in sum, Tijani, it is a context matter, but it is feasible because you have all those documentation requirements.

With respect to the point made by [inaudible], the GDPR is about individual private data that is correct, yet the distinction between corporate data and private individuals data is not always easy. So, there is jurisdiction in Europe according to which company name that allows for identifying an individual.

For example, my law firm is called Rickert Law Firm. Although it's a GMBH, it's a corporate entity, it still allows for my identification and that would make my personal data corporate data. There is certain risk involved in making a distinction between company data and individual data based on the self-assessment because the self-assessment might not accurately reflect what's required by law.

TIJANI BEN JEMAA: Thank you very much. Before giving the floor to Olivier to ask his question, we have questions on the Adobe Connect. Yesim will read them. Yesim, please? Yesim, do you hear me? Okay, I give the floor to Olivier to ask his question. Olivier, go ahead. Olivier? What happened.

GISELLA GRUBER: We are just getting Olivier on the phone line. Please bear with us for a second. Thank you.

OLIVIER CRÉPIN-LEBLOND: Yeah. Can you hear me now?

TIJANI BEN JEMAA: Now yes.

OLIVIER CRÉPIN-LEBLOND: Thank you, Tijani. Staff had muted all the lines and I didn't remember all the lines were muted. Usually I mute on my mobile, not by using *6 and *7. *7, by the way, for everyone is to unmute.

Two questions. One to Chuck and one to Thomas. First, thanks very much for this webinar. I think it's so topical. I've really pushed for participants in Europe to take part in this as we are, as one could call it, in the middle, in the center, in the real core of the cauldron and it's heating up pretty fast.

The question I have for Thomas is actually with regards to this cauldron. We have a date, as you mentioned, which is only a couple of months away for the GDPR to come into effect. You've mentioned that this doesn't mean that fines will be served the day after or on the same day. This needs to be weaved into local legislation. How long do you expect that time to take to go into local legislation and how long do you expect ICANN and ICANN registries and registrars to be ready to implement whatever we decide on doing, or whatever is decided on being done? As we all know, there's going to be a lot of discussion at the next meeting in Puerto Rico. But, then, once we've got – if we've managed to get consensus, then there needs to be implementation time as well. Is that a really huge task? That's the question to Thomas.

Whilst Thomas prepares his answer, I can ask a question to Chuck with regards to the RDS. I've heard – in fact, I've learned – that some registries are already doing open data RDS pilots. What's your feeling on these? Why would the RDS Working Group need to continue work? Can't we just go straight to implementation and check out how the RDS pilot works in parallel with the WHOIS? If it works well, just drop the WHOIS and here we are in the new vehicle.

THOMAS RICKERT: Okay. I guess it's my turn first. Olivier, thank you very much for your question. I have to say I'm afraid that you misheard my statement about transforming GDPR into national laws. This is not true for regulation. So, there is a risk of being sanctioned as of May 25th. Whilst I think that there are other companies that are collecting personal data big scale that are higher on the risk of data protection authorities to go after.

I do know that there are user groups who frown up ICANN's WHOIS system or many years that are just waiting to challenge the registries and registrars and that will likely not hesitate to go after the supervisory authorities for inaction if they choose not to pursue the cases.

So, actually, we don't have additional time. The opposite is the case. Even if ICANN's registries and registrars decided on a model in the morning, it would be too late for registries and registrars to implement the technical changes. Some of the players have development lifecycles of at least half a year, so some of them have already started implementing solution without even knowing what the end game with ICANN would be because they would know that if they only learn about ICANN's requirements in Puerto Rico or later, they wouldn't have a chance to implement that technically.

Maybe I can also use the opportunity while I have the floor to respond to a few comments that have been made in the chat about GDPR versus other data protection laws and that GDPR would only be applicable to European data subjects. That is true, but I think it's GoDaddy who have carried out some research on other national data protection laws. I think they've looked into 60 or so jurisdictions. The outcome of that was if you are compliant with GDPR, you're pretty much compliant everywhere.

I think South Korea might have quite harsh requirements as well. But, yes, it would be possible for operators to do something specifically for those who are governed by GDPR. But, let's just imagine if we had likely 60, 70, 80 different data protection regimes around the world or groups of data protection regimes. If we wanted the operators, registries and registrars, to come up with different solutions, they would need to be developed for all these markets.

So I think, from an operational point of view, it would make an awful lot of sense to look at the highest common denominator and have one solution that can be used at the global level in order to avoid fragmentation of the marketplace.

TIJANI BEN JEMAA: Thank you very much, Thomas. Can you please read the other question?

OLIVIER CRÉPIN-LEBLOND: My second question? Is Chuck on?

CHUCK GOMES: Yes. Olivier, thank you. There seems to be another discussion going on. Do you want me to answer Olivier's second question?

TIJANI BEN JEMAA: Yes, please.

CHUCK GOMES: Thank you. Olivier, I believe the pilots that you're talking about or the beta test, whatever they're being called by the various contracted parties, my understanding is those are related to the RDAP protocol. It's important that everyone understand the difference. We need some lines muted, I think.

It's important that everyone understands the role of the protocol versus the role of policy. The protocol is a technical standard that's been developed by the IETF, the RDAP protocol, and registries and registrars are already required going forward to use that protocol, although they don't have to be using it right at this moment.

So, the working group looks very favorably on the fact that these beta tests and pilots are being done by different contracted parties because it will test out the use of the protocol. It's a done deal that the RDAP protocol is going to be used in the future. Of course, the RDAP protocol, one of the big features of it, it allows gated access that Thomas talked about and that is part of the charter for the working group.

The fact that people are testing the protocol in no way limits the need for policy development because the protocol isn't policy. The use of the protocol may be policy, but the protocol itself is not. So, there needs to be policy to define, for example, how gated access would be used using RDAP. I know we're out of time I think, but hopefully that answers your questions. If not, please let me know either on this call or send me an e-mail.

TIJANI BEN JEMAA: Thank you, Chuck. Yesim, please.

YESIM NAZLAR: Thank you, Tijani. We have a couple of questions in the question and answer pod. I'd like to read them off. [inaudible] Alfredo Calderon's questions because he is first in the queue. He has a couple of questions.

What [inaudible] like AlfredoCalderon.com? Also, shall I read them or would you like to take them one by one, the questions?

CHUCK GOMES: One by one, please.

TIJANI BEN JEMAA: One by one, yes.

YESIM NAZLAR: This was the first question from Alfredo.

CHUCK GOMES: Let me respond, and Thomas, feel free to jump in. First of all, we need to be clear that nothing is going to happen to domain names that are registered because of GDPR. The domain name is registered. What needs to change to comply with UDRP requirements and the domain you mentioned obviously is personal information, so it comes into play with the GDPR, especially if the registrant is a data subject in Europe.

What needs to change, if it is in the European jurisdiction for GDPR, the display of any data associated with that domain will need to change. Today's WHOIS, which shows everything in WHOIS unless they're using a privacy service or proxy service, would show at all. That would, as I think Thomas has made very clear, would violate the GDPR.

TIJANI BEN JEMAA: Thank you, Chuck. I would like to ask you please to make a very short answer [inaudible] ten more minutes and we are almost over now. The second question, Yesim, please.

YESIM NAZLAR: Second question, from Alfredo Calderon as well. How does this effect [inaudible] Facebook or sites that use cookies?

TIJANI BEN JEMAA: Is this a question related to GDPR? Can we have the next one also?

YESIM NAZLAR: This question is for Chuck from Alfredo Calderon. Chuck, will the Next Gen RDS PDP be in place by GDPR's deadline?

CHUCK GOMES: No.

YESIM NAZLAR: Okay. The next question, again, from Alfredo Calderon. Does community work to enhance the GDPR requirement? Let me continue with the other questions. I think they're all relevant. What happens if in the future an outside EU organization serves an individual or entity outside EU? Sorry, from EU.

TIJANI BEN JEMAA: This can be answered by either Chuck or Thomas.

THOMAS RICKERT: The question was about a company outside the EU serving somebody inside the EU. In that case, it is, depending on whether there are just occasional EU citizens or EU data subjects that are served. If you are outside the EU and you're primarily having customers from non-EU customers but they're only sporadic EU customers, you don't need to be compliant. So, there's a little exception to the applicability of GDPR. But, if you are, for example, targeting European customers with your offering, then you need to be fully compliant.

YESIM NAZLAR: The next question is from Mohamed Yusef Alhaj. He is asking how can you apply penalties on organizations that is not within EU territory?

THOMAS RICKERT: So, I guess that's one for me again. I mentioned earlier that non-EU companies need to appoint a representative in the EU and that is for communication with the authorities as well. So, that can be used for sanctions, but then the other mechanism would be mutual assistance agreements where they exist, or vehicles such as privacy shared between Europe and the US, which also has a mechanism in there so that sanctions can be applied extraterritoriality.

TIJANI BEN JEMAA: Okay, next one?

YESIM NAZLAR: Thank you so much. The last question is from Vladimer Svanadze. Vladimer is asking what about non-member states of the EU, similar Georgia, where is association agreement with the EU and [neighborhood] [inaudible]?

THOMAS RICKERT: GDPR would be applicable to European member states and to I think members of the European economic area that have respective agreements with the EU. I am not sure at this point about the status of Georgia with this. But, the general principle that I mentioned, if a company from Georgia would serve customers in the EU and if this is not just an occasional customer, then GDPR would be applicable.

TIJANI BEN JEMAA: Thank you very much, Thomas, and thank you [inaudible]. I have a small question for both of you. You surely have seen the blog of the [inaudible] about the [inaudible] models that he proposed. Do you think that those are the only possible models? And if you think that they are [relevant] models, which one will you choose? There are four models: 1, 2a, 2b, and 3.

CHUCK GOMES: So, Thomas, I'll let you go on this one. I think it's much more suited for you.

THOMAS RICKERT: Which one of the models? I would pick none. I think they are all flawed. Sorry for being that direct. All the models, as ICANN mentions, are based on some principles that are applied to all the models, one of which is that all data that's currently being collected is collected under the new model. I mentioned earlier that I am convinced that admin [see], billing [see], tech [see] are not needed, in that unless there are further requirements that would be a violation of the principle of data minimization.

So, that prerequisite or that principle that governs all the three or four models makes all models flawed because the models only look at the disclosure part, but not at the collection part and other parts of the data processing.

Also, these models take for granted that all data can be passed on from the registrar to the registry, and I think that also wrong assumption, as I mentioned in my presentation, it is possible that the data can be transferred from the registrar to the registry level, but there are further legal requirements to be followed in order to make that compliant.

I'm afraid I'm not the only one with that gloomy view on what ICANN has proposed. I've been at a high-level meeting on Internet governance hosted by the European Commission yesterday and the representatives both from the Commission as well as from member states have asked the ICANN representative, Jean-Jacques Sahel, why these models have been proposed and that they think that the models even contravene the legal advice that ICANN has solicited from the Hamilton Law Firm.

CHUCK GOMES: Just to add, maybe to answer another part of the question, Tijani. That is are there other models? The answer is yes. In fact, ECO who Thomas is with, has proposed one that apparently wasn't really considered very much before ICANN developed the three models. I'm sure there will be other models in the future.

YESIM NAZLAR: Tijani, we cannot hear you if you are speaking.

TIJANI BEN JEMAA: Do you hear me?

YESIM NAZLAR: Yes, we can hear you now.

TIJANI BEN JEMAA: Okay. Thank you very much. Thank you very much, Thomas and Chuck, for this very good presentation and for this wonderful discussion. I would like to continue with you much more, but we are 17 minutes behind our time. We have a small part of our webinar that [inaudible] evaluation questions. Yesim, can you please go ahead with the evaluation questions?

YESIM NAZLAR: Of course, Tijani. Our first evaluation question is: how was the timing of the webinar? Is it too early, just right, or too [inaudible]? Please cast your votes now.

I'm moving on to the second question. The second question is: how is the technology used for the webinar? Is it very good, good, sufficient, bad or very bad? Please cast your votes now.

Moving on to the third question. Are the speakers the most [inaudible] of the topic? Is it extremely strong, is it strong, is it sufficient, weak, or extremely weak? Please cast your votes now.

Moving on to the fourth question. Are you satisfied with the webinar? Extremely satisfied, moderately satisfied, slightly satisfied, or not satisfied at all? Please cast your votes now.

Moving on to the fifth question. [inaudible]? Is it Africa, is it Asia, Australia and Pacific Islands? Is it Europe? Is it [inaudible] Island? Or is it North America? Please cast your votes now.

I'm moving on to the sixth question. How many years of experience do you have in the ICANN community? Less than one, one to three, three to five, five to ten, or is it more than ten years?

Finally, I'm moving to the last question. What topics would you like us to cover for the future webinars? Please type your answers in the allocated place and don't forget to hit the button next to it, so we can receive it. I'll keep this question open.

Back to you, Tijani.

TIJANI BEN JEMAA: Thank you very much, Yesim. For this question, please send us your topics or write them down here. We need them because we need to know what you are interested in for future. Thank you very much. I would like to tell you that there is now going on a webinar about GDPR and I encourage you to go and follow it. It is for four hours and now we already used, I don't know, [inaudible] minutes. Please go and follow it. It is very useful.

Thank you very much. Thank you, Chuck. Thank you, Thomas. Thank you, our staff. Thank you, our interpreters. And thank you all for coming to this webinar. This webinar is adjourned.

**[END OF TRANSCRIPTION]**