CLAUDIA RUIZ: Good morning, good afternoon, and good evening, everyone. Welcome to the At-Large Capacity Building webinar on the topic of Extradited Policy Development Process, EPDP, on the Temporary Specification for the gTLD Registration Data Team, Phase 2, taking place on Monday, the 6th of April, 2020 at 20:00 UTC.

We will not be doing a role call as this is a webinar, and if I could please remind everyone to please state their names before speaking. I'm sorry. If I could please remind all participants on the phone bridge as well as computers to mute your lines when speaking to prevent any background noise and to please state your name when taking the floor, not only for the transcription purposes, but also to allow for accurate interpretation.

And if we have Spanish, English, and French interpretation, as well as real-time transcribing in English. And I will provide that link in the chat below. Thank you all for joining and I turn the call over to Joanna Kulesza, the Co-Chair of the At-Large Capacity Building Webinar Group. Thank you very much. I turn the call over to you, Joanna.

JOANNA KULESZA: Thank you very much, Claudia. On behalf of Alfredo and myself, thank you for joining first in a series of webinars. It's coordinated, organized by Hadia Elminiawi who, in fact, is leading a small sub group on capacity building and webinars. Thank you very much, Hadia, for setting this up. I know we have a plan of a series of webinars. This is the inaugural one.

I’m very happy to be able to open the series to welcome everyone and thank you for taking the time to join us.

Over the next 19 minutes, Hadia and Alan will give us an update on the EPDP process. I can see in the list of participants, we have many ATLAS III ambassadors. The ATLAS III exercise was too large and focused on the EPDP as an example of how the policy process within ICANN community is being developed. For those of you who participated, who followed our webinars that we organized as a lead-up to the ATLAS III meeting, this will be an update. For those of you who are quite new to ICANN policy development, the EPDP is an exciting process, quite challenging but at the same time, very interesting, very [inaudible] that it’s an attempt to fit the global framework of the domain name registries and registrants into a local privacy policy [inaudible] and introduced a while back.

As already said, it is an exciting topic. It is a challenging one. And at the same time, At-Large has been tremendously lucky to be represented by Hadia and Alan who have devoted large amounts of time and passion and interest and knowledge to making this policy development exercise as fruitful and as easy for us at At-Large as possible. With that again, my thanks to both our speakers today for taking the time and again, agreeing to give us an update and share their interest and their passion and their experience on this, likely, most challenging quality development exercise we have placed within ICANN since quite some time. We’ve had challenging topics before but this one seems to take the cake in the last five years or so. So thank you very much for agreeing to give us an update on those. And again, thanks to Hadia for setting up a series of webinars and choosing the topics carefully. I am certain there will be a chance for us to update you on our further plans.

Without further ado, I am going to hand the floor over to Hadia if you want to open this specific webinar, then the floor is yours. Hadia and I also know that Alan will be the first speaker. So I'm leaving the floor to both of you. If Hadia wants to give us a brief welcome, you're more than welcome to do so. If we're headed straight into the presentation I see already displayed, then I will be happy to give the floor over to Alan. Thank you, everyone, for joining. I'm looking very much forward to this serious and this inaugural webinar specifically. Thank you.

HADIA ELMINIAWI: Thank you, Joanna. So definitely, we leave the floor to Alan. Welcome, everyone, to the webinar, At-Large Capacity Building webinar.

ALAN GREENBERG: And apparently I was muted. Can we have the first slide which is the agenda? Thank you.

I'll be going through the first part of this presentation, which essentially, is the history. This is the easy part and then turning it over to Hadia to describe where we are right now and the complexities of the current part. We'll be looking at the background and rationale for the PDP, how did we get here, what is this privacy legislation and how does it affect us. What happened in Phase 1 of the process, which took about a little over a year starting in October of 2018, if I remember correctly? And we’re now about a year and a half, two years into the process. I’ve lost track at this point. And we’re, in theory, close to finishing. Although, as you’ll see as we proceed, we maybe finished the EPDP but we’re not quite finished with the work. So there are some interesting challenges ahead. Next slide, please.

All right. Just a quick note at the bottom, you’ll see that we’ll be using the term WHOIS in this description for simplicity. The modern term that is used is either RDS which is Registration Directory Services, or more properly, RDDS, Registration Data Directory Service. For all intents and purposes, we’re looking at the same thing. WHOIS is also the name of a protocol, but it’s both the name of the protocol and an overall name describing the service and the data we’re looking at. So we’ll be using the term WHOIS, but they’re effectively interchangeable with the other terms.

So WHOIS is a database telling you who gTLD registrants are. It gives you the iden-… tells you who they are, their identity, how to contact them. In most cases, this information can be masked by a proxy service. So you can typically pay a fee of a dollar a month or something and ask the registrar to not reveal any of your information. That’s a service that has been offered for many, many years. Some people avail themselves of it. Others don’t.

The WHOIS, as it has stood until now, was required by contract with the registrars and the registries. That is, they were obliged to provide that information, and in fact, ICANN’s earlier agreements with the U.S.

government which have since expired, but those agreements explicitly called for support of the WHOIS protocol and database.

Public disclosure of information of natural persons ,and now we’re getting into buzz words, which may be new to some of you. Within privacy legislation, you refer to natural persons which are people and legal persons, which are effectively companies. So although the term “person” is used, whether it’s modified by natural or legal defines whether it is, indeed, personal information or information which simply is about a legal entity, which in most cases, is not protected by privacy legislation. Next slide.

Now, if you look at those two statements, you’ll notice that they’re in direct conflict with each other. You cannot require that all information about WHOIS be displayable, including contact information and names and numbers and addresses and phone numbers, and protect the information associated with natural persons. So that’s the quandary we were in. Now privacy legislation has been in place in many jurisdictions for a long time. And in general, it protects the, as I said, natural persons. Next slide.

Now in general – and I’ll tell you why I’m using the vague words – it does not protect legal persons. So if you’re a company, it does not protect your information. But what if, for instance, in your company, you use the name, Alan.Greenberg@gmail.com as one of your contacts and pieces of information? That suddenly is personal information. What if your company is called, in my case, Alan Greenberg Incorporated? Is that personal? Well, it’s not clear. Some jurisdictions say, “Yeah, that’s personal information. It’s my name.” Other jurisdictions say, “Well, you put that name into, your personal name into a company name, and therefore, in that context, it’s not protected.” So these things vary in certain jurisdictions and they’re interpreted differently by different courts. So there’s a lot of vagueness going around.

Now as I said, we have seen privacy legislation in many jurisdictions for a long time. To be blunt, it was largely ignored by ICANN. Some of our registrars and registries who were subject to this took this more seriously and there have been some provisions to allow for them to do different things. But in general, it wasn’t a major focus of ICANN.

What’s different? Well, the current legislation in Europe is the GDPR, the General Data Protection Regulations. And what’s different about GDPR is there are significant fines associated with it. Sorry. So, and what does significant mean? Well, it could be up to 4% of your gross revenue, not your profit, but your gross revenue. There are also provisions which could essentially stop you from doing business if you are in sufficient violation. So the monetary penalties are large.

Now presumably, you would not be assessed the maximum penalty for one minor violation. But nevertheless, since many of these businesses are not high margin businesses – certainly the registrar business is not a high margin business – a threat to a percentage of your gross revenue could easily wipe out all of your profit. So suddenly, it became rather important. Next slide.

GDPR is complex and highly technical. For those of you who might want to actually read the actual legislation, it’s readily available on the Internet. It’s many pages long and as soon as you get into it, you will be immersed in terminology which if you’re not already a privacy expert, a data privacy expert, then you will be a bit confused. There is the concept of controllers. Controllers are, in simple terms, those who set the rules. But it’s more than that. If you have a business relationship with someone, the fact that they perceive you as being in control, even if you’re not in control, may make you a controller.

Then there’s processors who follow instructions of other entities and the whole concept of in ICANN and in the WHOIS data, who is the controller is not clear. You can make strong arguments for saying ICANN sets the rules, therefore, ICANN is the controller. You can make strong arguments that the registrars are the controller. You can make arguments that we’re joint controllers which is a technical term and you can also make arguments saying we’re individual controllers. And in fact, for every piece of data depending on how it is used, you could have multiple different controllers for that same data. So it’s a messy subject.

You have to have purposes for processing data. So if I’m going to ask you for your phone number, I have to have a reason for asking for your phone number and I should not be asking you for information which I don’t really need to conduct the business that you’re asking me to conduct.

Now if you give me information, I have to keep it private maybe. Some information that you may give me may only have meaning if I make it public and you are obviously giving me permission to make it public or you wouldn’t be dealing with me at all for that particular use. Other information you may expect me to keep private but I might reveal it to someone if they have a sufficiently strong reason for needing that information. And I have to balance your need for privacy against that person’s need to access the data.

In these days of the Coronavirus, there is some interesting discussions going on if does violating your privacy in the name of improving public health, is that a sufficient reason for violating privacy? And different jurisdictions have made different decisions on that based on how much they value privacy over the public health, for instance. So it’s not an easy subject and it’s not something which is necessarily constant over time.

Due to the penalties that we’re talking about, those who are potentially liable – that is, their businesses are at stake – clearly have a reasonable reason for being very conservative. Let’s not take chances. Those people who want data and the kind of reasons you might want data for are to protect your intellectual property. If someone else registers a domain name and is masquerading as your company, or masquerading as you, you may have a reason for wanting to know who that is that’s masquerading as me. If you are protecting, doing cyber security work, and people have registered domain names explicitly for phishing or for a number of other cyber security issues, you may want to get hold of them. Moreover, if someone as stolen your domain name and is using it, the cyber security people may want to get hold of you to tell you someone has stolen your domain name. So there’s good reasons for wanting to be able to contact people. And all of this came into effect as of late May 2018. Next slide.

So now look at ICANN. We have a deadline of May 2018 and we’re not ready. We still have on our books, policies which says registrars and registries must publish all the information they have. The registrars and registries are going to be potentially liable and ICANN, for that matter, might be potentially liable for large fines, if indeed, they follow the rules.

Now ICANN policies are normally set by policy development processes within the gTLD world, PDPs. PDPs are a multistakeholder process where various people from around the community, including At-Large, can discuss the issues and try to find some middle ground that they can agree on. Now we were in a situation where there was no time to establish a formal policy. People were liable to huge potential fines if we didn’t change the rules. Luckily, there is a provision in our contracts which says the ICANN Board can set policy in urgent situations and this was deemed to be urgent. But there’s a catch. It can only set policy for one year. The presumption when we wrote those contractual clauses many years ago was that in a year, we can easily come up with new policy.

Well, the reality is the PDP rarely can come up and put in place new policy in a year. That’s virtually impossible. We may develop it, but it’s not going to be implemented. Now in our contracts, the contracts that ICANN has with its registrars and registries have a base contract and they have a number of appendices, of addendums, and these are called specifications. So a contract may have ten or 15 different specifications to give the details of some part of the contractual relationship. The Board enacted a Temporary Specification. That is a specification which would be added to all of the contracts, but would be temporary for one year. And that’s the source of the rather confusing name “Temporary Specification”, just says it’s an extra part of the contract but it’s going to go up in smoke in a year. Next slide.

And we have a quiz. The quiz is “Why was the Temporary Specification established to replace WHOIS?” And can we have the quiz on the screen?

CLAUDIA RUIZ: Are you [inaudible] the quiz?

ALAN GREENBERG: We’re ready for the quiz.

UNIDENTIFIED MALE: No, I’m not on the [inaudible].

ALAN GREENBERG: No, no. No, you’re now on the previous slide. Somehow staff has to do some magic to bring the quiz up so we can see the possible answers. I think that’s what’s supposed to happen. There we go.

And we have two questions. We’re only looking at Slide 8. So why was the Temporary Specification established? We have four possible answers: because specifications can never be permanent, because the Board had nothing better to do, current rules about WHOIS were potentially legal, or all of the above. If you answer and then we’ll proceed.

Question for staff, do we normally… How long do we normally allow for this?

CLAUDIA RUIZ: I could end it now. One moment.

[CHERYL LANGDON-ORR]: Was anyone able to submit? Because there were two questions and we’re only answering one.

ALAN GREENBERG: We’re only answering the first one.

[CHERYL LANGDON-ORR]: And therefore, the submit button did nothing because this is waiting for both questions to be answered.

ALAN GREENBERG: Ah, I didn’t even notice there was a submit button. Can we have the quiz back again?

CLAUDIA RUIZ: Yeah, Alan. Sorry to interrupt. So the following is that the quiz was done as a continuation so in the meantime, I can adjust it to see if I could fix it. But as of right now, it’s going to continue.

ALAN GREENBERG: Okay. Can you adjust it by the time the next quiz is ready?

CLAUDIA RUIZ: We have four slides. I’ll try my best.

ALAN GREENBERG: Okay. All right. We’ll come back to this quiz.

CLAUDIA RUIZ: Okay.

ALAN GREENBERG: Next slide, please. All right, so we’re now at the place where the Temporary Specification was enacted. So you can wipe your forehead and say, “Okay, we’re not going to be fined this month but we now have about a year in which to make this better.” And as I said, establishing a policy in a year is rather difficult in ICANN. But we only have a year.

So a PDP was established, an Expedited PDP. That is one with a different set of rules to allow it to proceed, hopefully at a faster speed. The normal PDP traditionally in ICANN, pretty much anyone who wanted to participate could participate. In earlier PDPs many years ago, the number of people who could participate was very limited, specifically limited to the GNSO Council or its people, and it was, a bunch of years ago, it was widened so other people could participate. This one was changed so it can have participation from all parts of ICANN that wanted to participate but a very restricted number of people and the number of people was based on which group you belong to, and I won’t go into the algorithm used. And it was limited in size both to make sure that there were balanced views and to make sure that there weren’t an infinite number of people who could prolong the process just allowing everyone to talk. So it was a new process. It was an experiment. Next slide.

And we’ll fast-forward now to the Phase 1 results. The Phase 1 results were done in under a year. So we made that target and essentially, the resultant policy was familiar, what was similar, generally, to the Temporary Spec. But there were many, many changes made to it. Most personal data is being redacted because just as with the Temporary Spec. But in addition to that, as with the Temporary Spec, the Temporary Spec allowed registrars to also redact the information on legal versus companies and that was maintained by the EPDP into the policy.

The EPDP, rather GDPR, has geographic limitations. Essentially, it protects those in the European Union. There are extra territorial aspects to it, that is companies, other places, might have to protect things as well. But it generally protects under certain geographic regions. The Temporary Spec and the EPDP policy allowed registrars and registries to not differentiate between geographic regions. And disclosure, if someone had a reason for asking for data, it was highly decentralized. That is you had to go to the registrar or registry and ask them for the data. And as you would expect, the results were variable. Next slide.

Now, this slide is the getting into the section that Hadia will be doing on access and disclosure. Now we had significant debates in the EPDP on whether what we were talking about is access or disclosure. From the point of view of the person wanting access, wanting some data, it was getting access to it. From the point of view of the contracted party who was holding the data, it’s disclosure. So there are two sides to the same thing but we had literally hours of debate on which word we should use, and finally, the wisdom of the Chair said we’ll use both. And so we’re now in a situation where we talk about access and disclosure.

Third parties can have a legitimate need to access redacted data. That is personal and nonpersonal data. Experience with the decentralized model that came out of the Temporary Spec and out of the initial policy is that it was not satisfactory. There were rejections where the requester deemed it to be unreasonable. There were completely ignored requests. That is you made a request and you never got an answer or you might get an answer three months later.

The situation was sufficiently awkward that we even had data protection officers in Europe, that is those who were clearly well-versed in what data protection law was and because they had gotten a complaint about something else, they wanted to access WHOIS information and they went to a registrar and the registrar said, “No, we’re not going to give it to you.” So we were in the perverse situation that we were being more, the contracted parties in some cases were being more rigid than the data protection officers in protecting privacy. So clearly, that wasn’t working very well and the real challenge was how do we put in place a system that will allow legitimate people to get access to data, but at the same time, protect the privacy that is owed to the individual data subjects.

And now we have a quiz and we will patiently ask. Are we ready for the first quiz and then the second? We are. And can we go back to number eight, the first quiz that we missed? Or did we skip it?

CLAUDIA RUIZ: I skipped it. I need to add it. I can add it right now while you’re doing that.

ALAN GREENBERG: Okay. We’ll do this quiz first and then go back to the previous quiz. This quiz is, “Why was the EPDP Team for the Temporary Specification for gTLD registration data established?” So why do we have an EPDP Team? It’s number one, to replace the Temporary Specification with formal policy. Number two, to create RDS policy that meets contracted party needs. Three, to create policy that meets users’ needs, or four, all of the above. Select which one you think it is and hit submit. If you don’t hit submit, it won’t work.

And the majority of people answered “to replace the Temporary Specification”. And in fact, the correct answer was “all of the above” because we were trying to clearly replace the Temporary Specification and result in a policy which met contracted party needs, i.e. protected them to make sure they weren’t going to be held liable, and at the same time, made sure, try to make sure that legitimate users, legitimate people can get access to data that is legal under GDPR.

Do we have the first one ready or should we come back to it later?

CLAUDIA RUIZ: I’ll come back to it the next section, please.

ALAN GREENBERG: Okay. All right. Next slide, please.

All right. So we now come to Phase 2 of the EPDP and that is to build, essentially, design a Standardized System for Access and Disclosure, SSAD. So the concept is we would have a single location to submit requests. So if you needed data that was not public, that was redacted, you would go to a specific place to ask for that data. There would be standardized ways of asking for it. It would be reviewed. Now I’m giving you partly the design and partly the outcome because during the discussions, there were many other variations that were looked at. But this is where we’ve basically ended up to and Hadia will be going into the details, in far more detail than this. But this is the basic overview of what we ended up with.

There would be a standardized way of review and response process. So when you submit a request, it would be checked for completeness. If you omitted a field, it was rejected until you just submitted again. It would log it. So if you've made a request, we now know how made it and when it was made.

We would have to find out who you are because number one, we need to know and understand who we're giving data to. That's a requirement under GDPR. But more important, based on who you are, there may be certain characteristics that we know about you. You might be doing this for cyber security reasons. You might be law enforcement who might have special privileges. So based on who you are, you may be treated differently. That doesn't mean you have automatic access to any data. There are a few cases where you do have automatic access, but those are very, very restricted. But based on who you are, we may know something about you.

And funding is a crucial issue. How are we going to pay for this? Clearly, there has to be some cost born by the users but there may be costs born by others. More important, funding may vary. Not funding. Pricing may vary so we might give law enforcement a different price than intellectual property people who are doing this, essentially, as part of a business. We may price things differently for cyber security people. So the fees and funding is going to be a very integral part of this process and it's very hard putting costing together when you have no idea, or pricing together when you have no idea what it's going to cost. And at this point, we have no idea what it's going to cost or what it's going to look like. So it's a real challenge. Next slide.

So it’s going to be a cent-… At this point, we believe it is going to be a centralized system run by ICANN. The SSAD will accept requests only from accredited requesters. It will authenticate, validate queries. In the general case at this point, the SSAD will then send the query to the contracted party, the registrar or registry, to review it and possibly approve it and to reply. The reply will come directly from the registrar which avoids problems of transported data flow. If it had to go through ICANN, then there’s the issue of can it flow back from wherever it is into the U.S. and then to the user. So the response is coming directly from the contracted party. And if, indeed, there is personal data involved, now remember, we are redacting, in many cases, information on legal persons. So there may not be any personal information involved and it may be that the data should be released immediately just because privacy legislation does not require it not to be required. But if it is personal information, then you must do a balancing test. You must look at the reason the requester is asking for it and balance that against the needs of the individual involved, the registrant, for privacy.

Now many believe that that has to be done by a human being. There is belief by some that some of those might be able to be done in an automated way. We are currently having a very small number of cases where we believe the SSAD itself can say there is no question the data needs to be released, and simply send instructions to the registrar or registry to release the data. And the SSAD will log everything, including when the contracted party releases the data. They will log the fact that it has been released so we can end up with performance statistics and know just how well this is working. Next slide. I think that’s now a quiz.

Who can submit requests to the SSAD? And the possible answers is anyone who knows the right URL, only those who are formally accredited, only those who can afford to pay, or none of the above.

And the vast majority said “only those who are accredited” and that is the correct answer. Now only those who can afford to pay may apply to some people, but for other entities, there may in fact be no charge so that’s not the general answer.

Can we go back to the first quiz now if it’s ready? Now this is a challenge. We’re going back to stuff that was done 30 minutes ago. If we’re not ready, then let’s just skip it. There. No, we’re looking for Slide #8 questions. All right, let’s just skip it and we’ll go on to Hadia’s part. We’ll come to the first question at the end. Hadia, I’ll turn it over to you and enjoy.

Can we take the quiz down and go on to Slide #16 please?

HADIA ELMINIAWI: Are we taking the quiz now?

ALAN GREENBERG: No, we’re going to you.

HADIA ELMINIAWI: Yeah. Okay.

ALAN GREENBERG: And we’ll come back to the first quiz at the very end. And Hadia, I apologize. Our plan had been I was supposed to stop at every, before every quiz and ask you if you had any comments, and I forgot. My apologies. I hope you didn’t have too many comments.

HADIA ELMINIAWI: It’s fine, Alan. I did not have any comments. And to summarize, after a user has been accredited, the requester can submit a request to disclose nonpublic registration data to the Standardized System for Access/Disclosure. The request would typically contain information like the domain name pertaining to the request, a list of data elements requested by the requester, and the legal rights associated with it, in addition to a request type like is this an urgent request, for example.

Following the [inaudible] of the disclosure, the Central Gateway Manager, which is the entity within the Standardized System for Access/Disclosure, that would be actually responsible for receiving the request and sometimes making decisions. So after the Central Gateway Manager receives the request, it [inaudible] information that has been provided and all of these [inaudible] contain [inaudible].

CLAUDIA RUIZ: Hadia?

HADIA ELMINIAWI: Yeah.

CLAUDIA RUIZ: So sorry to interrupt but the interpreters are having trouble hearing you, I believe. Could you move your mic or something?

HADIA ELMINIAWI: Okay. I'll do that.

So following the receipt of a disclosure request, the Standardized System for Access/Disclosure will confirm all required information provided and all of this is done in an automated manner. If the required information is incomplete, the Standardized System for Access/Disclosure would provide an opportunity for the requester to amend and resubmit the request.

When the information is complete, the SSAD would respond with an acknowledgment response and would look into the request. If it is one of the use cases that has been deemed automatable, the central Standardized System for Access/Disclosure will make the decision whether to disclose or not. The central gate… And if the decision is actually to disclose the data, the Central Gateway Manager will ask the relevant contracted party to disclose the required data elements to the requester.

Up until now, we have only two possible cases for automation. The first one is just regard to requests from local law enforcement or applicable jurisdictions, and the other one is with regard to responses to Uniform Domain-Name Dispute Resolution Policy providers or Uniform Rapid

Suspension providers for registrant information certification. And even now, this is not quite certain and we have been discussing it quite a bit. But anyway, that’s what we have right now.

So if the request is not one of the agreed upon cases, which are only two cases now, the Central Gateway relates the request to the contracted party, as Alan mentioned before, and may provide a recommendation to the contracted party whether to disclose or not. The contracted party may follow this recommendation made by the central gateway, but if it does not, it must inform the Central Gateway Manager about the reason for not following the recommendation so that the system learns and improves on future response recommendations.

So the experience gained over time with requests and responses is expected to improve the decision making and recommendations made by the Central Gateway Manager and by the contracted party. Also, the data available in relation to the number of requests and their types is expected to help improve the agreed service level agreements. If we could have the next slide please.

So therefore, a mechanism that allows for the evolvement of the system without the need to conduct a PDP each time an improvement is added, is essential and is required. And again, up to now, we have not agreed on such [inaudible] mechanisms. We have been discussing this a lot and I hope we can reach something in this regard. The contracted parties may request a Central Gateway to automate all or certain types of disclosure requests. If we could have the next slide please.

So it’s a quiz. Who is responsible for making the decision to disclose the data to the requester within the Standardized System for Access/Disclosure? If we could have the answers on the… Yeah. So it’s the SSAD itself, the registrars or registries. When we say the SSAD itself, it's the Central Gateway. So the Central Gateway Manager is actually responsible for making the decisions with regard to some automated cases and for receiving, also, the requests. The registrars and the registries, there’s no decision necessary, if you opt to get it, all of the above, none of the above.

Yeah, the right, the correct answer is all of the above. Well actually, as we said, there are two cases. If it’s an automated case, then the Central Gateway would respond to it, would make the decision. If it is not, then the registries, the relevant registry or registrar will do that. Sometimes if it contains no personal data, then it could be actually disclosed. And could we go to the next slide please?

So the next slide is about accreditation. So we mentioned before that in order to be able to use the system, you need to be an accredited user. So what is accreditation? Accreditation is an administrative action by which the accreditation authority declares that the user is approved to gain access to the system. The accreditation authority will basically confirm and verify the identity the user of the system. It will give the requester some kind of credential like a username and password. Those credentials identify the user and can be used by the Central Gateway Manager for validation purposes, can be used by SSAD for validation purposes.

The accreditation authority will also give the user some sort of assigned assertions or credentials. Those assigned assertions or credentials will convey information such as the purposes of the request and the legal basis of the request. So the identity credentials have assigned assertions attached to them. There will be only one accreditation authority managed by ICANN and ICANN may work with third party identity providers that would verify the identity of the requester and manage the assigned assertions. If we could have the next slide, please?

So again, the accreditation alone does not ensure disclosure of the data. It only allows the use of the system. The decision to disclose or not still lies with the Central Gateway Manager and the contracted parties. The accreditation only facilitates the decision of a disclosure as it confirms the identity and legal basis of the requester. Nevertheless, each request is examined on its own merit by the Central Gateway Manager or the contracted party. Could we have the next slide please?

The accreditation authority can revoke the accreditation of the users. Such cases could include prerequisites for accreditation no longer exist, the user abuses the system. I note here also that the accreditation authority will be audited. So all accreditation activities such as the accreditation request, information about the basis on which the decision to accredit or verify the identity was made, all of this will be logged by the accreditation authority and identity providers. So if we could have the next slide please?

It’s a quiz. What is the role of the accreditation in SSAD? To extract money from requesters, to ensure who we know who is asking, to aid in understanding why the requester needs the data, all of the above, none of the above.

If we could have the results please. Okay, so to extract money from the requesters. Okay, that’s not a target but that’s happening because accreditation is actually not for free. To ensure who we know who is asking, yes of course, to confirm the identity of the requester. And also, remember that accreditation also provides assertions with regard to the purposes and legal basis of the requesters. So it’s also to aid in understanding why the requester needs the data. So the correct answer is all of the above.

ALAN GREENBERG: I should mention that the use of “extract” was deliberately there as a slanted word.

HADIA ELMINIAWI: Yeah, so it’s definitely not to extract. Yeah, but it is for fees. So that’s not a purpose, but yeah.

So the response time. So as noted before, when a requester submits a request to the system, the information provided includes a request type. Like, for example, if it’s an urgent request, that’s a priority one, or if it’s a UDRP or URS, it’s a priority two. All other requests are priority three. So urgent requests, according to the, what we currently have in the report, the requests are, the response is received in one business day. That means that if you actually submit a request on a Friday afternoon, you could get the response on Monday. And urgent requests are defined as circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure online or offline. An example of online is Root Server attacks. Offline, an example for that is a bank or an electricity system, something like that. So again, those urgent requests do require urgent responses.

And again, after the system comes in to operation, and we have data that tell us more about the number of requests and their types, how many are urgent or how many are a priority two or priority three, that’s what actually helps us in determining meaningful service level agreements. Again, this is one of the reasons we require an alternative for the system to improve. If we could have the next slide, please.

Okay, so it’s about open issues. So [inaudible] is a hybrid model to improve. That’s still an open issue and it’s being discussed. But again, it is essential, actually, to have an efficient system because, again, we cannot have a current, meaningful service level agreement system now because we don’t have the data that would permit us to put this in place. Also, we have been able only to automate to [a pay] system. But after the system comes into operation, most probably it would be obvious that some more cases need to be automated. And that’s helpful not only to the requesters because they receive their answers quickly – and the answer, by the way, does not have to be yes; it can be no – but it's also helpful to the contracted party.

And then another open issue is [inaudible] versus legal [inaudible]. And during Phase 1, we concluded that registrars and registry operators are permitted to differentiate between the same legal and natural persons but they’re not obligated to do so. We have also concluded that ICANN Org will undertake a study to consider the feasibility and costs, including both implementation and potential liability costs of differentiation between legal and natural persons. Also, examples of industries or organizations that have successfully differentiated between legal and natural persons look into privacy risks to registrants, look into potential risks to registrars and registries. Accordingly, ICANN Org put a short questionnaire, put forward a short questionnaire to collect input on the risks, feasibility and costs of differentiating between legal and natural persons, and the report is expected to be shared with the team in May 2020.

But again, the EPDP Team has not been able to reach any kind of consensus in this regard and the recommendation currently is to consult the GNSO on if and how it is expected to consider the findings on this topic, is to consult the GNSO on the steps forward in this regard. So we haven’t reached any conclusion and the GNSO who will actually look into this.

The other topic that [inaudible] important and also, we haven’t reached any conclusions in relation to it is accuracy. So GDPR does not define the word “accurate”, but the Data Protection Act of 2018 defines “inaccurate” as “incorrect or misleading as to any master of [inaudible]. A principle quality of the GDPR seeks to [inaudible] accuracy of the data. According to the Information Commissioners Office, GDPR includes [here] proactive obligation to say [inaudible] to delete or correct inaccurate data. So actually, we do see this as an important topic and within scope. The GNSO has deemed it, has deemed accuracy within scope but due to the time limitations, the EPDP Team is not going to discuss this further and the Council is expected to form a scoping team to further explore the issue in relation to accuracy and accuracy according [to the system.]

So those are the important issues that are still open. The first one is not closed yet. The second and the third are closed. If we could have the next slide, please.

So what does GDPR protect? Any data stored in a computer, any data submitted to the corporations, any personal data such as your name, address or age, data associated with domain registration. So yeah, that’s the correct answer, any personal data such as your name, address, or age. So any personal data, name, address, phone, e-mail, biometrics records, Social Security number, data on place of birth. It’s basically any data that can be used to distinguish or trace an individual’s identity. This is what GDPR protects.

So thank you so much. I’m finished here and we’re open to discussion, if we could have the next slide, please.

ALAN GREENBERG: Well, if we could go back to the first quiz.

HADIA ELMINIAWI: Yeah.

ALAN GREENBERG: I demand my quiz be done. There we are. Who is the Temporary Spec… Why was the Temporary Specification established to replace WHOIS? Because specifications can never be permanent, because the Board had nothing better to do, current rules about WHOIS were potentially illegal, or all of the above. And the correct answer was, indeed, the current rules were potentially illegal.

And before we open the discussion, if we can go back to Slide 24. I will note that all of these are from the ALAC’s point of view based on our earlier discussions we’ve had and earlier statements are exceedingly important. And how we respond to the results of the PDP are going to depend heavily on to what extent the mechanism is, indeed, developed that we think will work, what the final outcome is on legal versus natural and accuracy. These are all issues that I think the ALAC is in a position to say we can’t live with the results if these are not addressed suitably. And as Hadia mentioned, at this point, the recommendation in the draft report is that we do effectively nothing about the last two and defer it back to the GNSO to be handled perhaps sometime in the future or not. So it remains to be seen just how the, what the final report says and how the ALAC responds to it.

And let’s open the discussion. Anyone have any comments or questions? No hands being raised. We might end early. Joanna, please go ahead.

JOANNA KULESZA: Thank you, Alan. And Hadia, thank you for the most informative presentation. We had a few questions in this chat. I'm not sure you guys were following the chat. I noted down a few questions coming from Rick Lane. I think they were targeting specific slides and were aimed at specifying the information that you had provided. I'm wondering if you guys would want me to read them, whether Rick might want to repeat them for the purposes of the discussion, or whether they might have been answered by further discussion.

ALAN GREENBERG: I certainly was not looking at the chat. So I haven't answered it. I don't know if Hadia or someone else has.

HADIA ELMINIAWI: No, I didn't read them either. Maybe Joanna, you could read them out.

JOANNA KULESZA: Okay. I will try reading them out. If I miss anything, Rick, please feel free to raise your hand and specify.

So the first question was a kind request for defining law enforcement in local or otherwise applicable jurisdictions. I believe that is something that came up on one of Hadia's slides. Holly attempted to answer, indicating that that is an issue in itself, and Rick followed up with a question on who makes the decision on accessing personal data, who makes the ultimate decision. I would like to stop here because I think those two questions go hand in hand, so to speak, if you guys want to pick them up.

ALAN GREENBERG: Okay. I can try.

JOANNA KULESZA: And then I have a few more coming from Rick. Alan, go ahead.

ALAN GREENBERG: Thank you. Law enforcement, typically, if you, for instance, are a registrar in Germany, then you have a legal obligation to respond to law enforcement, to certain kinds of law enforcement requests in Germany. If you get a request from someone else in another part of the European Union, there may be certain agreements where you have to respond. But if you get a request from someone in the U.S., for instance, there are no guarantees that U.S. law enforcement can demand that you release something if you don’t have an office in the U.S.

So typically, U.S. law enforcement might go through German law enforcement to get to you but you are obliged, essentially… The rules get very complex. But at a first simplistic point of view, you respond, you only have a legal obligation to respond to law enforcement in the jurisdiction in which you exist. So that’s what we mean by law enforcement and local jurisdiction. And law enforcement within your jurisdiction has certain rights that other law enforcement somewhere else might not, probably doesn’t have. So the question about…

UNIDENTIFIED MALE: So Versign…

ALAN GREENBERG: Sorry?

UNIDENTIFIED MALE: I was going to say, so Verisign and GoDaddy don’t have to respond to the Europeans because they’re U.S.-based?

ALAN GREENBERG: If they have an office in Europe, then they may have to if that group is approached. That starts getting into areas that are past my level of expertise. But in general, you can establish for any given registrar what law enforcement they are obliged to respond to automatically. And even then, there has to be the appropriate paperwork done and things like that.

In terms of who makes the decision, that’s a really complex question. In general, the controller has to make the decision but as I pointed out in one of my earlier part of the talk, it’s not clear who the controllers are in every case and there is a case to be made why ICANN is the controller and if ICANN makes the decision and that decision is found to be against privacy legislation that ICANN would be fined. There are arguments why the registrar or registry is the controller and they would be the one who would be fined, and there are cases where both of them could be fined or have penalties. So that's… If we had that answer easily, we would not be spending all of this time. If we knew definitely that ICANN was the controller, then ICANN could make the decisions and it would not be an issue of liability for the registrars and registries.

RICK LANE: My question is to the poll that asks for… It said all of the above were the ones making the decisions and you can't have all of the above. I think Holly made that point as well.

ALAN GREENBERG: No. Okay.

RICK LANE: If all of the above are making decisions and there's conflict in the decision, then there must be someone who makes the ultimate decision in [inaudible] poll.

ALAN GREENBERG: Yeah. No, I can address that. The answer is depending on the request, it may be one or the other or no question at all. In other words, for some classes of data, there may be no… If it is known, and the if is a big question, but if it is known that it is not personal data, it can't be released, period. There is no balancing test to be made. If it is data that a type of request, as Hadia mentioned, that we've already decided can be automated, then the SSAD will make the decision. And in the general case, it will be the contracted party. So all of the above does not apply to every request but any given request might be any of the three.

HADIA ELMINIAWI: And if I may add to it, that please note that when we talk about law enforcement from the same jurisdiction, we are talking about the automated disclosure. Remember we had two types, when the Standardized System for Access/Disclosure [inaudible], it’s [inaudible] into the request for. If it is a request that we have declared automatable, that means that this use case can be responded to in an automatic fashion.

And in this case, the Central Gateway Manager would actually respond to the [inaudible]. It would make the decision and the decision can be a yes or a no. If the decision is a yes, then it requests the contracted party to release the data. And up to now, we have only two use cases for that. That doesn’t mean that other law enforcement from other jurisdictions cannot make the request. They actually can make a request, but it won’t be an automated one. So when the Central Gateway looks at the request and it’s not a request from the same jurisdiction or an equivalent law enforcement agency, it directs the request to the contracted party and the contracted party looks into it and decides whether to disclose or not.

And one important [inaudible] here that law enforcement, that governmental entities would also have accreditation authority. But this accreditation authority would be based in the territory or country itself and it would be responsible for accrediting the governmental entities so that they can actually access the Standardized System for Access/Disclosure.

Also, I see a question also by you that says, can the contracted parties make registrations natural persons? Well, technically, what's happening that they're not differentiating between natural persons and legal persons. And that's one of the problems that if the organization feels that there is an organization [feels], even if this feels it has data in it, they are not sure that the registrants actually identified himself correctly. So you can say that what's currently happening, that most registrations are natural persons even if they're not. And that's one of the issues with actually, one of the [playing] issues for making this differentiation.

JOANNA KULESZA: Thank you, Hadia. If I may try and attend to the questions. We have a few more questions from Rick. I have them all noted down. But I also see Joan's hand is up. If Rick would like to address those questions himself, I'm happy to give you the floor, Rick.

ALAN GREENBERG: Why don't we go to Joan first and let her get her question and then go back to Rick?

JOANNA KULESZA: Perfect. Let’s try and do that. So Joan, we’ll start with your question and I have a few more from Rick noted down. If he would not like to read them out, I’m happy to read them out for him. Joan, the floor is yours.

JOAN KATAMBI: Thank you so much, Alan and Hadia, for your great presentation. And I also want to thank the team behind the [inaudible], Alfredo and Joanna. So I need an inquiry from Hadia. Looking at the response time, does it matter if they’ve received over 1,000 queries or issues for the response [inaudible] that it all [inaudible] that it’s actually one day or it doesn’t matter. And if you get one query or 1,000 queries, those two get response at the time she has actually specified. Thank you.

HADIA ELMINIAWI: Okay. Thank you for your question. So currently, this one business day does not speak to the number of requests. So whatever the number of requests they receive, as an urgent request, they need to, according to the Service Level Agreement, they will need to respond to within the business day, the one business day.

Our argument is that urgent requests, one business day could be too long and then that 24 hours is more appropriate. But the contracted party’s response is we do not know yet the level of request or the number of requests that we are going to receive as urgent requests, and that we cannot commit to 24 hours because we don’t know the volume that we are going to receive. So currently, it’s one business day for any number of urgent requests.

ALAN GREENBERG: Yeah. If I can add something, the urgent requests are ones threatening life or limb or things like that. So we're not expecting huge numbers of those. But the current Service Level Agreements that are proposed are, number one, will not even come into effect until we have some time and then are graduated. And moreover, they're not an absolute demand, but essentially, an average. So they have been built quite flexibly right now and it is, it's well understood that we're going to have to look at what's going on and adjust them as we go forward. But you can't not have anything because then there are no ways to take action against registrars who don't answer at all, for instance.

Joanna, back to you.

JOANNA KULESZA: Great. Thank you both. I think those were our most comprehensive answers. We see praise in the chat room and I'm happy to share those. Those were most informative answers and most informative presentations.

ALAN GREENBERG: Okay. We do only have ten minutes left, so we'll try to be brief with our answers.

JOANNA KULESZA: Indeed. I’m looking at the clock. I’ll try to read the questions coming from Rick. My understanding is that those are more of a conversation-making questions but I will go through those and I will let you reflect on summarizing the meeting.

So the first one is – I’m reading out the question – if all of the above are making the decision, again, deciding on access, who has access to the information on the identity provider to make the ultimate decision? Won’t the sharing of that [PII] be a violation of GDPR? That’s the first question. The second one, I think, is easier, an easier one. What is the timeline for this to be completed? And the third one, who has access to the information one the… Oh, apologies. We already have that one. So those would be the three questions. Who has access to the information on the identity provider? And what is the timeline for this to be completed? Those are all the questions that I managed to catch in the chat box if you guys want to address them. Thank you.

ALAN GREENBERG: I think the question is who has access to the information on the requester, not the identity provider.

JOANNA KULESZA: That’s what it says in quotation marks. So you guys might be [inaudible].

ALAN GREENBERG: Yeah. Certainly, if the requester is a natural person and has information about natural people, it is protected by GDPR and other privacy legislation. So there will be a whole set of rules of who can get access to data from the SSAD but that’s over and above who can get access to data from the WHOIS or RDS data. So it’s certainly private and we’re having discussions right now to what extent should we be making public, for instance, that a requester, whether it’s a personal, a natural person or a legal person, should we be releasing that information? Or is that, indeed, private?

And clearly, we’re going to be doing a lot of reports, some public, some not. But privacy of the requester is also an issue that will have to be considered during the implementation of this. In terms of the timeline, it’s a really good question. We don’t know. We’re still working on what the system will do. There’s obviously got to be some design done. A lot of the functions that we’re looking at are things that ICANN or similar, or other bodies we work with, already do to some extent. So we’re hoping that it can be adaption of some things and not inventing everything from scratch. But simply establishing the accreditation process to find out who is it that will be able to accredit intellectual property lawyers or trademark professionals or cyber security professionals and then building the process by which we establish. In the case of cyber security, we’re going to have to establish what the credentials are. Not just everyone can claim to be a cyber security person. That’s going to take time. So I’m guessing if we could get everything up and running in a year, it would be glorious. I doubt if we will. But we don’t know the timeline, to be blunt.

UNIDENTIFIED MALE: Hello? Hello?

HADIA ELMINIAWI: I just wanted to note one thing in relation to the identity provider. So as [inaudible] back to the accreditation authority and identity provider, all of this would be logged. The logged data shall be disclosed where disclosure is considered necessary to fulfill an applicable legal obligation of the accreditation authority or the identity provider. I do read Rick’s question. It says, “Who has access to the information on the identity provider to make the ultimate decision?” I’m not quite sure what he means by that, but if he means logged information or… Again, if we are talking about logged information, it’s only disclosed in relation to legal obligation or auditing requirements.

JOANNA KULESZA: Thank you, Hadia, and thank you, Alan, for those answers. I heard someone trying to get through. If there is one more question from the audience, we are happy to take it. I don’t see any hands raised and I think we covered all the questions.

ALAN GREENBERG: I see a question from Gg Levine right on the screen.

JOANNA KULESZA: I thought that was the one that Hadia attempted to answer, but I’m happy to give you the floor, Alan, to take that one. Go ahead.

ALAN GREENBERG: Maybe I missed that. Do we have any concerns about end user safety in light of limited access? In other words, do we believe that the redaction of data is impacting users? I think that’s the question that’s being asked.

And the answer is that’s why we’re here. We believe there are significant issues for the non-registrant user and there are several billion non-registrant users compared to hundreds of thousands of registrants. WHOIS is being used in cyber security investigations and including things like spam filters for a long time now. And the inability to access some of that information now, we believe is significantly impacting users. Every user, pretty much who uses e-mail has the benefit of spam filters. Anyone who uses a web browser has the benefits of various safety and security features built into these browsers that use information that’s collected on websites and on domain names to say whether you can trust them, whether they are ones that may give you vulnerabilities. So yes, we believe end users are and will be significantly impacted by the inability of cyber security people to take appropriate actions because of this redaction. So that’s, and in particular, the fact that GDPR has been over-implemented in redacting a lot of information which is not required to be redacted, that does make the contracted party’s implementation a lot easier. But we believe there is significant impact of that. Thank you.

JOANNA KULESZA: Thank you very much, Alan. I think it’s, in a sense, a wonderful summary of this webinar that brings us back to policy development. Thank you for taking the question and thank you for asking it, Gg. I’m wondering if our speakers have any final comments or summaries. We have three more minutes. I am looking at the clock.

If that is not the case, I am happy to thank you, everyone, for participating. Special thanks and applause to our presenters today. Thank you for taking the time again to help the community better understand where we are, where we’re headed and where this entire process is coming from.

On behalf of Alfredo and myself, I sincerely hope that you guys found this exercise useful. We’re always standing by for questions and suggestions and special thanks to Hadia for setting up this specific webinar and for planning ahead for further webinars. Stand by for upcoming announcements and different themes to be discussed, including SubPro, including DNS abuse, including geopolitics. So this is first in a series. Thank you, especially, for making this interactive, this initiative to have us being quizzed throughout the webinar was particularly useful to make sure that we are able to follow on all the information that is being presented.

And with that, thank you, everyone. Thank you to all our interpreters. Thank you to our staff and see you during the next webinar that will be set up by the At-Large discussing specific themes that are of interest to end users. Thank you, everyone. This meeting is adjourned.

ALAN GREENBERG: Thank you, Joanna.

[END OF TRANSCRIPTION]