ICANN76 | CF – GNSO: RYSG GeoTLD Group - NIS2 Impact on the Registration Proc
Saturday, March 11, 2023 – 13:15 to 14:30 CUN

DEVAN REED: Hello and welcome to the RySG GeoTLD Group NIS2 Impact on Registration session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, questions or comments will only be read aloud if submitted within the Q&A pod. I will read them aloud during the time set by the chair or moderator of this session. If you would like to ask your question or make your comment verbally, please raise your hand.

When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at a reasonable pace. Mute your microphone when you are done speaking.

This session includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real-time transcription, click the "closed caption" button on the Zoom toolbar.

To ensure transparency participation in ICANN's multi-stakeholder model, we ask that you sign into Zoom sessions using your full name. for example, a first name and last name or surname. You may be removed from the session if you do not sign in using your full name.

With that, I will hand the floor back over to Nacho Amadoz.

NACHO AMADOZ: Thank you very much, Devan. This is Nacho Amadoz. We organized this session from the GeoTLD group in order to start discussing what should be the approach that we need to take internally for the upcoming implementation of the NIS2 directive. But then we thought this is something that we could share with the whole community so that we can see whether we find areas where we could collaborate or could start discussing what could be the best way not to make this more complicated or not to create the incentives for a disaster that could happen if we have God knows how many different implementation regimes. So that's why we thought let's discuss this as early as possible within the ICANN agenda and bring on board as many people as possible. So thank you to all those who are attending the session remotely or present.

We have a panel of experts that are going to be discussing certain topics. We have Elena Plexida, Vice President of Government and IGO Engagement of ICANN. We have Thomas Rickert, which is a member of the GNSO Council and Director of Domains and Numbers—domain names and numbers at ECO. Right, Thomas? Thank you. And we have a Amadeu Abril i Abril, which is CORE's Chief Policy Advisor.

The session is going to be conducted in the following manner. First, we are going to get an update from Elena on the status or how we think is going to proceed with the NIS2 implementation—and if I'm saying things that are not correct, please just go ahead and correct me—followed by a discussion within the panel but also completely open to participation from anyone. So please, just go ahead, raise your hand. We'll try to keep it orderly. But we are happy to embrace chaos as it couldn't be otherwise.

We have some questions. And I think that we are going to get to them to guide the discussion after the presentation from Elena that will help us set the framework in which this discussion is going to take place. So with that, thank you again for attending the session. And over to you Elena.

ELENA PLEXIDA: Thank you, Nacho. Hello everyone. Really nice to be sitting in an actual panel and close to people. I'm still not used to it, to be honest. Okay. some introductory remarks. Honestly, I tried to while doing the introductory remarks answer the first question of this panel which was: will there be an impact on the registry day to day things? So in the next slide, just a very high-level NIS2 at a glance.

Of course, we all know it amends replaces the existing NIS2 directive. Member states will have to transpose the directive by October 2024. There are also implementing acts foreseen that the European Commission has to put forward and there are guidelines for the European Commission and ENISA to put forward.

Let's remember NIS2 is part of the cybersecurity package of Europe, meaning that it's all about cybersecurity measures and reporting obligations.

So, if we're here to debate what might be the effect on registries, I think it will be, while we want to discuss mainly the registration data part, it will be an omission not to mention that part two.

So we have cybersecurity measures with emphasis on the supply chain. That's on the next slide. We have reporting obligations for significant

effects. We have also deadlines for reporting—24 hours, for example, for early warning, 72 hours for initial notification, one month for final report. And importantly, these things, the cybersecurity measures and the reporting obligations, are accompanied with fines. If a registry is not established in the EU, but offers services in the EU, they have to put in a representative in the EU.

And when it comes to the cybersecurity measures and the reporting obligations for registries, the European Commission has to specify them for DNS operators and registries by October 2024. So we will have to wait and see apparently what will be the impact, particularly for registries that were not captured in NIS already because as we all know, NIS already covered the DNS operators, but it was up to the member states to see within the jurisdiction to say "okay, this is essential" or "this is not essential". Now, everything is automatically essential.

I am told—I'm not an expert here—that the cybersecurity measures are not something crazy. [inaudible] operators [inaudible] themselves more or less do these kinds of things. Maybe the supply chain emphasis is something to be attentive to. The reporting, probably it will add some administrative burden. Again, we'll have to wait and see.

Now to the important part of this debate: the registration procedure. Next slide please. Okay. Obviously, if we were to answer the question, will the day-to-day registry business be impacted by NIS2? The answer is they will depending on how different the implementation of NIS2 requirements will be compared to the existing practices of the DNS operators.

When it comes to gTLDs, remember, of course, NIS2 now applies to ccTLDs and gTLDs. When it comes to gTLDs, this means it will depend on how different the NIS2 requirements when implemented would be with the existing practices of DNS operators. For the gTLD space, this means it depends on the extent that—and I'm now quoting NIS2—standards developed by the multistakeholder governance structures [on the] national level are taken into account. This is something that we find in recitals in NIS2 itself. In other words, to the extent that the policies developed by the multistakeholder model and then applied in the contracts are taken into account. Again, that's for gTLDs. And we should reflect on the fact that the member states have to implement a law for all gTLDs doing business in their jurisdiction, while respecting the uniqueness of their ccTLDs. It's the same law, it's now here.

So let's look very quickly at the NIS2 requirements. And I'm sure my fellow panelists will have lots to add on those parts. Data collection, NIS2 lays down a list of data to be collected. Honestly, they read like a minimum set of data to be collected. Will member states opt to put in place a comprehensive list? In principle, that's not the idea, but again, in principle.

Publication of legal persons' information. According to ICANN community policies, registries are not required to differentiate. But they can do so if they choose. That's the outcome of the EPDP Phase 2A.

Now, NIS2 says in a recital that email can be published as long as it does not contain personal data. That's the same thing that the European Data Protection Board had told us. I'm sure you remember. It also says you have to publish at least the name and the phone number. Again,

we'll have to wait for the implementing laws. Apparently, [I] will have to say that throughout.

Access. Here we have requirements for registries to provide access upon lawful and duly substantiated requests by legitimate access seekers. They have to reply within 72 hours. That might be a challenge for registries. I don't know. My fellow panelists will say.

Now with access, which is a sore point, if you will. Assuming the registries could, by the implementing laws, rely on 6.1c GDPR, instead of 6.1f that they rely GDPR nowadays, it could be an improvement, but here I'm just assuming. It seems that the NIS2 recognizes 6.1c for the specific purpose of ensuring the security and stability of the DNS, which in turn contributes to the high common level of cybersecurity across the Union. So, again, [to be seen].

Interesting to note I think is that the European Commission can put in place guidelines with regards procedures for access. Again, NIS2 says that such guidelines if put forward should take into account to the extent possible the standards developed by the multistakeholder governance structures.

Finally, verification and data accuracy, which I suppose is one of the most important parts for the registries. Now, accuracy nor verification procedures are defined in NIS2. But we have recital with comparatively—specific and comparatively dynamic rather—requirements that could, depending on the implementation, again, become a moving target in the future. It says it should reflect the current best practices used within the industry. And also the progress made in electronic identification. Again, to be noted on the part of verification.

Although NIS2 does not provide specific guidelines regarding which methods to be employed to verify at least one means of contact of the registrant, the European Commission, as I'm sure you have all seen, has announced its intention to launch a tender for a study on current good practices. It mentions analyzing use of Know Your Customer technologies, or EID, or machine learning technologies. As the publication itself says, the intent is to inform the implementation of NIS2. So this publication seems to be setting a rather high standard, potentially. And I will stop here with the intro. I hope you were able to hear me. Thank you.

NACHO AMADOZ: Thank you very much, Elena. I don't know if any of the two other members of the panel want to address any of these definitions that she has indicated or we should start with the questions to guide our discussion.

What I noted regarding the last bit, which is this tender to define, following know your customers and all these languages, the concern that we may have to see if this is going to be receiving our feedback or if we are going to be able to come up with our feedback that shows some degree of harmonization between registries and registrars as to how this should be implemented in order to avoid these differences in implementation. I think that's one of the main concerns that we have.

This solution could be also something to worry about or to try to inform. That is one aspect. But the other is the number of solutions that we are going to be finding in the different jurisdictions and how they are going to be affecting us. As we said in the beginning, we thought that this

could be an idea to start discussing how we go about this, if we try to get together one single solution, one set of guidelines for the feedback that we need to provide in this process, so that they are heard and that we avoid the solution being defined without our intervention. And I guess that's the guiding principle of this session. What do you think, Thomas, for example?

THOMAS RICKERT: Thanks very much, Nacho, and hi, everyone. Thanks, Elena, for the excellent overview. I do not know whether everyone in this room or attending remotely is an expert in what NIS does. So maybe for context, I should make two or three introductory remarks to shed some light on where we are because this is a directive and not regulation. You might have vivid and probably fond memories GDPR was introduced, which was a regulation, meaning that is it is directly applicable. So you have to take a look at the GDPR and hopefully you find out what your requirements are.

Here we have a regulation that needs to be transposed into national law—a directive, I'm sorry—and that needs to be transposed into national law. And we don't yet know what the national lawmakers are going to make out of it. So we might end up with a situation where you have different requirements. Or in a worst case scenario, as many different national requirements as we have member states in the EU. And we have quite a lot.

The other thing is that in order to form a view on how an industry—a very diverse industry … As we know, we have CCs, and then amongst the Gs, there's also some variety—how an industry should respond to

these legal requirements. It would be good to understand what the requirements of the lawmakers are.

However, if we take a look at NIS2, it doesn't clearly say what it wants from us. And I think part of that is because the laws aim at not being concrete and for individual cases, but they shall be abstract and general. That's the way lawmakers come up with things. And that doesn't really help. I mean, I think that European lawmakers had the best intentions. They said, "Well, we wanted to help ICANN in particular, after all these discussions around the EPDP and the SSAD and the legal uncertainties to get some solid legal basis for what they're doing." But if you step back a little bit, we had huge discussions around natural versus legal and we had huge discussions about the application of the GDPR and when disclosures are in order and when they are not okay.

What NIS2 basically says is data of legal persons needs to be published as long as it doesn't contain natural persons data. So that doesn't help a single bit because that's exactly the discussion that we had in the EPDP. So we're left alone with that. No guidance whatsoever.

And then when it comes to disclosure requests, it says everything in the NIS needs to be governed by the GDPR. So we need to do the GDPR tests again. So it doesn't necessarily help with that either.

Now, one good thing—and Elena mentioned that earlier—that the lawmakers plan or they require national lawmakers to come up with a legal basis according to 6.1C. That was on one of the slides. 6.1C means that in this catalog of legal bases for data processing, you have one clause (and this is 6.1C) that if you process data to fulfill statutory legal requirements, then you must do that. So we are waiting for this

statutory legal requirement in order to guide us in terms of how we should process data. And then we can if we do it in accordance with these newly crafted laws that we are therefore going to have. But it may well be that the national lawmakers do it differently, all for themselves. So that's an issue.

Also, there's one big issue that in the very last minute, they've introduced this what is now 28 subsection six, which says that there should be no duplication of collection, so that we don't have things both at the registrar as well at the registry level. But collection is just one of the processing activities that we have. Collection is one, transfer is one, alteration of data is one, deletion of data is a processing activity. So does that mean that if the registrar collects, it can then be still transferred to the registry or does that mean that if the registrar collects that, if we take the principles of privacy by design and privacy by default to heart, which is also mentioned in one of the recitals as one of the guiding principles, shall we actually apply data minimization and if the registrar collects and verifies data, then it's okay, then we don't need to pass things on to the registry?

So these are unknowns, which is why we as an industry should come up with information to guide GAC reps in our environment, as well as the national lawmakers on how to come up with something meaningful, that causes least disruption and friction, fragmentation in the marketplace. Because imagine it's going to be a nightmare for registries to respond to these different legal requirements, but it's going to be a nightmare for registrars as well because then users might end up putting a couple of gTLDs and ccTLDs into their basket case, and all of them have different requirements for validation. Then they get emails

from folks they have never heard of because they think they liaise with the registrar. And suddenly something comes from the registry. So it might be a nightmare.

And I think if we're doing all this in order to stimulate the commercial activity in the member states, we should make it easier for users foremost. And this is not something that set out to make it easy. And therefore, I think we should try to come up with something guiding the lawmakers to make it as consistent and as easy for everyone. But we do know that CCs love their independence and rightfully so. But nonetheless, we should keep the level of friction as low as possible in order to make it for everyone as easy as possible to comply.

I have much more to say, but I think I've spoken too long already, so I should stop here. But I know that I'm Amadeu manages to squeeze like five times as many words into the same time. So I'm sure that you go next, right?

AMADEU ABRIL I ABRIL: I'm sorry. Where's the microphone? Here. I'm Amadeu Abril. Nacho, I'm not sure what are the other questions because I don't see the agenda. But perhaps at this point [we had] a couple of things here regarding the directive and some good and bad points to add to what Elena and Thomas said about what risk.

First, in this directive, we are the exotic guests. This is not about us. This is about critical infrastructure, blah-blah-blah. Look, DNS. Sure. Important. Let's put something. Right? But the rest of the directive, it's quite exotic to our lives, to a certain point … I mean, Elena mentioned

at some of the cross reaches regarding security things. But at the end of the day, for instance, for geos that are the organizer of the room, in most of the cases, this is more for the backend registry providers than for themselves. For the ccTLDs, it's different. But still, this is not about the TLDs. And DNS is like a guest, as I said, here.

Then second thing. This directive is not very good. When I was working on the European Commission in the prehistory, before anybody knew what was the Internet, including me, my boss told me that I could tell whether a piece of legislation of the EU was good or bad—EC at the time—by counting the proportion between articles and whereases. He said if it has double or more than double whereases than, articles it's bad. This has three times whereases.

For instance, there is one article regarding domain names and 10 whereases. These 10 whereases have been written in different times by different people. How we know that? Because it's a mess. I mean, the first two refer to TLD registries and DNS service providers. Then the next four refer to TLD registries and other entities that provide domain name registration services and the last four to all of them. But that's important, because the first one refers to the scope. it says TLD registries but not registrars, for instance, or other entities. The second one is even more important, 84. And this is the first thing you need to show to your GAC representative or the ministry department that's dealing with that. 84 says, important part, TLD registers, DNS is global, etc. They should be regulated in a highly harmonized way. So put that in front of them, right?

But this is for TLD registries, not for other entities providing domain name registration services. For instance, registrars. And that's important. I represent CORE here. CORE stands for Council of Registrars. We are an association made of registers and from the registrar point of view, this directive is not as good.

My advice, first thing, let's not go just registrars here, registrars there. Look at, for instance, Article Six. It's even worse in the definition. What's this, entities providing other—providing domain name registration [services? A long name.] It's registrars. It's written there. Proxy services providers [inaudible]. It's resellers. Now what in Hell is a reseller? We'll come back to that.

But then it says that in the definitions. We go to Article 20, we go to whereases 109 to 117 except 115 that doesn't deal with this. And it says things like registries and entities providing domain name registration services will do things like collect information—sure—publish the information. Resellers … Resellers of resellers will need to have WHOIS. Provide access to the information when legitimate access seekers request something. Really? Resellers, how they will be found if they are not identified?

I mean indeed, in the WHOIS for gTLDs there is a field, an optional field for reseller. Just count how many domains in your TLDs have anything as content in reseller field. It's from zero to marginal, right?

And I'm not saying the reseller should not be taken into account, but the problem is, in my experience, reseller is anything. There are many resellers that in fact are companies that have a large portfolio of domain names and they sign up as resellers in any registrar. A law firm that has

registered 15 domain names for customer and they sign as reseller from a registrar, if we apply all these to entities as defined as also as resellers, these will explode. Because most of the resellers and the resellers of the resellers of the resellers are not operationally prepared to handle that.

And at the end of the day, the registrar is a legal construct—is a legal construct to have legal responsibility for an operational responsibility in front of the registry and third parties for certain things.

So another thing is please bring the registrars and … I have to explain that. One of the funniest thing you could do in Brussels in the '80s and early '90s was … I mean, every other year, there was a big convention named "What's a farmer." So they spent weeks and weeks there, thousands of people discussing what's a farmer because indeed the main two profiters from the Common Agricultural Policy were the Queen of England and the Duchess of Alba, who never seen a crop in their life, or a cow. So is that a farmer? It's a farmer if you have some rooms that you rent in summer, it's a farmer if you just buy cows to have milk, and to be paid to have the cows and to have the milk but not to sell it because there's too much milk in the market. All these things happen. [We're spending money.]

So now I think that ECO should start thinking about organizing "What's a reseller" in Brussels before they do the legislation, because I repeat, a registry, more or less, we know, a registrar, more or less, we know. Even if registrar are more different, including the ccTLD cases. Reseller, we don't know. And just passing all these obligations as if resellers were real professionals of domain name registrations with the technical operation knowledge would be a disaster.

Another thing that's bad here, and it was mentioned, the legal person, individual person, a mess, but something worse. It says for legal person, the email of the registrar should be published unless it contains personal information. How do you do that in an automated way? If I have ceo@eco.de, is that a role or it's, I don't know, Carlo Eduardo Orlandi who happens to be a person working there? I have no idea. The machines have no idea. So it means that we need to rebuild manually each email for a registrant of a legal person. I don't know how this works.

You probably have registrars that systematically have copied for the last 25 years the same information in organization name and registrant name. I can give you names of registrars who do that. How do we handle that? But especially, how do we handle these things that are very optimistic, like the email unless it has legal … So there are things that we need probably to convince them. But I think that the basic thing we need to do with government, just telling them, look, this is the minimum. Indeed, this is a directive. Don't go beyond that. Just don't go beyond that. This is enough.

And then a personal note, for Elena and for all of us attending ICANN, it's a little bit, I would say, strange reading this and finding three times the expression and that these are could—could, not should—could take into account to the extent possible what these people in Cancun are doing by the name of multi … What's the name exactly? Multistakeholder governance instances at the international level. This means ICANN. It's new name for ICANN apparently. Could take into account, but could not, indeed. To the extent possible. So I think that this is the danger. We need to explain what's being done. We need to

explain. Even the directive says, well, if you verify—whatever verify means—an email address for a contact, the magic thing of sending an email to a Gmail address and getting an answer, that's enough. All this for that? Really, all this for that? This is what we need? This is what we want? Yes, probably, because we don't have any good alternative. But don't let your government say, "I have something. The post office here will verify with a picture of the registrant and send that over …" A new technology somewhere, [easy for me,] whatever, let's invent something, and we'll send the information about the registrar. This is what we need to prevent, the very big ideas based on the buzzword of the week that will stay in legislation, will make our life impossible forever.

But the minimum of the directive that's not that bad, even it has some things regarding legal person and individual person that you don't understand.

Sorry, the last thing. What's a legitimate access seeker? I don't know. Because it says legitimate. It doesn't say privilege. For legitimate, including CSIRT, law enforcement. Indeed, they include that. But excluding others or not? If it doesn't exclude others, we'll have a problem because answering everything that's legitimate in 72 hours, regardless of the long weekends that we have six, seven times a week in Europe, that will be a problem.

And if I have a request from the police, at least I know what the police is in my jurisdiction. You have a request for intellectual property. Before I know, who is this guy, and whether this guy represents the trademark

holder or not, I have spent already a couple of days before looking at the concrete request, right?

So this doesn't work, 72 hours for all the requests. It works for the privileged actors, but they don't say that. They say legitimate, including … So it could be expanded by the national legislation and we need to make sure that the national legislations, legitimate means anyone who has a legitimate claim, period, because then we somehow will be unable to fulfill the requirements here. Okay, that's all for now.

NACHO AMADOZ: Thank you, Amadeu. I know you had your hand raised, Werner, but I think there are follow-ups from the panel first. Then after, you, so we don't move to the next topic without addressing the follow-ups.

THOMAS RICKERT: Great. So I just wanted to add two or three points after what Amadeu said with all the operation complexities that we have. What we heard from the Commission when they commissioned the study on DNS abuse that I think most of you will have read, they loved what some of the European ccTLDs are doing with their very harsh verification procedures. They see that they have virtually no abuse but ignoring the fact that they have a far easier time to do all the verification with the limited geographic reach and they might have registers or databases that they can go to in order to do that.

So there is a risk that the national lawmakers might say, okay, our ccTLD is doing well, so we might request the GeoTLD to just apply the same standards and we don't care about the other Gs. As long as we have a

victory to celebrate, that we in our little country have done everything that we can in order to make things as secure as possible.

And there is a danger to that, so we need to make sure the ICANN community stands united, regardless whether it's Gs that are open, whether you have nexus requirements or whatnot, because it's important that it's as easy as possible for folks to register domain names.

Even if we make things as secure as possible, it will always miss the mark to a certain extent, because as we know by now, more than half of the DNS abuse that we're seeing—and again, this is one of the driving factors for NIS—is through compromised domain names. And you can do all the verification and validation in the world that you want, you will not prevent that from happening.

Also, we know that you can fight DNS abuse very efficiently without knowing the PII of the registrant. So I think we always need to put things into context and say, well, you might be up for something because someone told you that this is going to be the silver bullet solution if you just have as much data on the registrant and make as much of that available. Ideally, as we had in pre-GDPR days when everything was wide open. But that's not going to make the place any safer. We need to work on other mechanisms in order to make sure that DNS abuse is responded to as quickly as possible and that ideally is prevented. But through Article 28 of the NIS, we're not going to see a lot of change. And I think that's also a message that we need to convey.

NACHO AMADOZ: Werner, over to you.

WERNER STAUB: My name is Thomas Rickert and I'm the registrant of the domain name cancuntaxi.something.

UNIDENTIFIED MALE: .sucks.

WERNER STAUB: Yes. No, cancuntaxi.official. Now, that is actually the level—

UNIDENTIFIED MALE: You look great today.

WERNER STAUB: Exactly. That is actually the level of our procedures. And that is the background for what we see in NIS2. It's literally the same level of flimsiness. I looked at, I didn't read the whole thing but I didn't find any decent use of the word identifier in the … There was talk about data. It is irrelevant to talk about data. The identifiers are key. And we're not going to correct the bad sides of this directive but we can sidestep the problems that it causes.

And one of the things is look at our own procedures. If we just don't know how to identify people because we just proliferate pointless identifiers by the millions—pointless identifiers in our own datasets. The only decent identifier that we have in the ICANN world is the ICANN registrar ID. That's just about the only decent one that we're using.

We're not even allowing people to voluntarily provide identifiers if they wish to—and many would actually wish to correctly identify themselves. And also, many would actually wish to prove that they are who they say they are. It is not like we need to force them. Most of the decent registrants would like to prove that they are who they say they are. They would like to distinguish themselves from the fly-by-night people.

So, I think if you look at this, we can look at all the problems that can be caused by our procedures modulo the NIS directives. This is just a big mess. If we want to build something that works, let us build systems of identifiers and use systems of identifiers that actually have the solidity. We mentioned LEIs for some time. It is one of the examples of identifiers with a level of decency. This actually anchored in law in the respective countries and it basically built on that. It is created by the financial regulators in mostly G20 countries. It is a decent identifier where you have one and only one identifier per party. Its point being to check that you don't get two, just like ICANN checks that the same registrar doesn't get two registrars for the same legal entity. They would at least have to create another shell company if they want to have another registrar or identifier.

So in the same way, we can create systems and we can share that I think in the context of the GeoTLDs. We are probably kind of in good companies because all kinds of associated with the local community, where people also like to have people identified.

NACHO AMADOZ: Thank you, Mexican Thomas. Volker, you're next, right?

VOLKER GREIMANN: Yes, thank you. Volker Greimann, CentralNIC. I'm not sure if I agree with Werner that most registrants want to identify themselves. Most registrants want their domain name as quickly as possible, without as much hassle. They want as few steps necessary to complete the order process and be able to use the domain name. But that's not the point I wanted to make. I think what we have in the ICANN ecosystem is some kind of a shift of responsibility. In the past, it was always the registrant obligation to provide correct and accurate data. This was entirely identified as a registrant obligation. We had to enforce that against the registrant if we learned that this information wasn't correct, but ultimately, it boils down to the registrant having the obligation to provide accurate, complete and up-to-date data. Now with NIS2, it becomes our responsibility to ensure that the registrant has done that. And I think that is part of the issue that we need to address as a community here as well.

Finally, with regards to the duplication of collection of data parts, I think that could be key in coordinating not just between registries and registrars but also between registries that duplication does not occur.

The worst scenario I could imagine is really that every registry does their own thing, and a registrant has to verify his data 20 times when you register 20 domain names across 20 TLDs. That is a horror scenario for every registrant, for every registrar, and the registries probably won't notice that much. But ultimately, it will cost them registrations, so it should be a horror scenario for them as well. Thank you.

NACHO AMADOZ: Thank you, Volker. I'm going now to you, Michael. But that is precisely the object of the session, in our view, which is to find which is the way we should proceed, get all together. And there are different ways to find the solutions. we could find in the past some things that some of us had to differentiate between legal and natural persons that had to disappear because of the effect of GDPR, that didn't incorporate any verification procedures. But at least we could make this distinction between legal and natural persons that could help weeding out where we need to go in some of the obligations, but that we understand that they don't have necessarily to be the threshold for everyone. So let's try to find if there is a way to get together to avoid this 20 different things for you to verify and process anytime you want to work with someone. Michael, you're next.

MICHAEL PALAGE: Thank you. Michael Palage for the record. So at a high level, I agree with almost all of the criticisms or critiques raised by the speakers. I think you have confirmed that this is not perfect, by any stretch of the imagination.

But Thomas, when you were speaking with Sally when she first presented to the council, you talked about do not let perfect be the enemy of good. And I guess I look at this more as a glass half full as opposed to a glass half empty. I look to ccTLDs that are trying to improve it and there are more. Within the last year, we've had India, we've had Australia. More and more doing it.

And to your point, while that may be on an individual country by country basis, within CENTR, there was a recent EU grant where four

ccTLDs tried to exchange this. And I guess what is concerning here is there's a lot of … I've heard a lot of today of what we can't do. I haven't heard anything of what we can do. And that to me, I think is the important driver to Amadeu's point is there's … I think when I read NIS, yes, they are trying to use code speak to ICANN. Yes, they want the multistakeholder model to work. But if it can't, they are clearly indicating they will do it. And I think that's the point here is let's come up with solutions. Again, ccTLDs I think are doing a much better job than most gTLDs are doing and hopefully we can focus the remainder of the time on what are the areas where we potentially can do something good, as opposed to just the critique.

NACHO AMADOZ: One second, Amadeu, before going to you. We had a set of questions that we discussed or we circulated among the panel to guide the way we wanted to approach this session and the last two of them are: are concerns about the fragmentation implementation real and what can the community do to avoid that? That's one. And the last one was what could be the next steps to assist national regulators to obtain or to achieve an adequate implementation regime? And that that is, I guess, where we need to go to see how we manage to get there. There can be questions about the substance of some procedures, but they can also be things as such as the ones that Thomas and Amadeu said saying, okay, we have several unknowns; we need to clarify what are these unknowns and we need to let them understand what is all this, where we are at, what are the complications that could be created for the agents intervening in the registration procedure? Amadeu?

AMADEU ABRIL I ABRIL: [inaudible] something you said regarding ccTLDs and gTLDs. I see all of them were the same—all the ccTLDs and all the gTLDs—and they are not. NIS is about security. It's not about identification. That's a tool. It's about security, right? And in domain name case, this comes very close to abuse and fraud, besides the security threats to the infrastructure. But the rest of this collection of data, etc., has to do with abuse and fraud.

And here the difference is not the level of identification. Not only and not mainly. The main difference also is the policies for the registries. This session was organized for the gTLDs. I know, most of them, it turns out that for the vast majority, the level of abuse they have not in total, also proportional to number of registrations, is very low compared to other gTLDs. Why? Not because they verify more necessarily, but also because of their policies. For instance, their [inaudible] verification or how they deal directly with abuse, instead of simply sending the ball back to registrars and see what happens, right?

So one thing to do regarding Nacho's question is show that everything is not just who you let into your TLD, or how difficult or how easy it is to get into your TLD but also which policies you apply regarding the use, the price, and how you react to abusers. And that makes a difference. And I repeat. I know many gTLDs that have very comparable or even lower levels of abuse than some ccTLDs in the same area.

DIRK KRISCHENOWSKI: Dirk Krischenowski from DotBerlin and DotHamburg for the record. Coming back to Michael's proposal and question what we can do, let me make a more radical answer in the direction where we are heading. Actually, the situation today is that we as registries get a very mixed data set from registrars. Many registrars just send redacted or proxy data to us, some full data. It's a mixed picture, but with a tendency to redact more data. So we have an incomplete data set anyway.

So I would say… And the duplication of the content, we would have to delete the data we get, or those data we get from the registrars in the future. So I would just say we don't care and we delete all the data we get from the registrars because of the duplication of the data. And that's it. That could be a proposal and it would be in line with the law.

NACHO AMADOZ: Because it wasn't clear to me. You're saying that our proposal could be that registries just get rid of any data associated with a domain name?

DIRK KRISCHENOWSKI: No. It was … Yeah, except that we have to deliver the CZDS data anyway, but this is not … It's a question if it's personal data associated with it. But I would say that is fine.

MAARTEN SIMON: It's Maarten Simon, SIDN ccTLD. It's an interesting proposal but it's never going to work because for ccTLDs it's very important to have the correct data of the registrants. So I can imagine the [idea] because I've thought about it too. But no, that's not going to work, because, in our

case, our countries, our governments think it's important for us to have this data and they will never let that [happen]. So not a good idea.

DIRK KRISCHENOWSKI: But then we have the clear separation of ccTLDs and gTLDs. Yeah.

UNIDENTIFIED MALE: Yeah.

AMADEU ABRIL I ABRIL: Wait a second. You have a community TLDs that need the data for their verification of the community requirements as well.

DIRK KRISCHENOWSKI: Amadeu, we are a GeoTLD and with requirements and many others of our GeoTLDs as well, and what should we do if registrars—major registrars like Ionos or OVH or others don't send us any data? We can't verify.

NACHO AMADOZ: Sorry, I think Thomas was first in line and then you, Marianne.

THOMAS RICKERT: Yeah, thanks very much. Let me get back to Michael's point from earlier. What do we have on the positive side of things? I think the commission, with this new law—or the European Parliament, they gave a clear hint that they want ICANN to play a role in this. So if they say standards should be used that have been developed by a multistakeholder or

global multistakeholder organization, that is ICANN, as someone has said rightfully.

So, in a constructive way, I think we should try to make the existing policies including the outcomes of EPDP work to meet NIS requirements. And also you might remember, at least those who have been at the table long enough, and there are some in the room, we went through this whole verification thing when the RAA 2013 was discussed. So there was a discussion at the time whether pre-validation should be done, whether domain names could be used before the validation has been completed. And the compromise struck at the time was that, yes, you can start using the domain name, and we take a look at one data element. And NIS2 also says one data element. So there's something in there where we can replicate what we already have.

That is the bottom line. It is perfectly possible for other for CCs to go above and beyond the requirements if they wanted to. But I think what we're looking for is a standard that can be applicable throughout the industry, with the least possible disruption. That doesn't mean that we have to fight against abuse, as well. So we shouldn't take away any energy from that. But we want to meet the legal requirements as they come. So advocating for those work products, I think would be a good idea.

And, Dirk, to your point about thin versus thick, it is correct that many registrars after the temp spec came out chose to just redact everything and they haven't changed that approach since. I think that what we're seeing in that regard is exactly what I mentioned at the outset, that we

have poor drafting of NIS, since this change of the in Article 28, subsection 6 came in in the very last minute.

So I think there should be room for registries to be thin, to say we don't want that data, we don't need it. But there might be others that need to check nexus requirements, that have eligibility requirements that they need to check and they might have a legal basis for getting the data transferred in.

This is a marketplace with a lot of variety in which we should allow for variety. But we should make it as easy as possible for everyone to be compliant with upcoming laws.

NACHO AMADOZ: Dirk, just hold on for a second, because first is Marianne and then Werner.

MARIANNE GEORGELIN: Hello, Marianne Georgelin from AFNIC. So, DotFR but also DotParis. So, ccTLD, gTLDs. It was just to say that it's not that new, making verification on domain names. What we realize at the central level, amongst the ccTLDs, is that we basically already do what is being asked. And I think for some of our gTLDs, the ones we're working with, it's already the case. We know how to make verification and it might depend on how we make an interpretation of this Article 28, to which extent do we have to make those verifications, but otherwise it also could be interpreted as, okay, let's check what we already do. Does it fit? Does it answer what is asked? And let's see if there is a gap or not.

So what I'm saying is that it might not be such a revolution, and maybe we can build on what we already do, because we have very good practices on this matter whether on ccTLDs or gTLDs.

NACHO AMADOZ: Sorry, there was next Werner, next Elena, next Dirk.

WERNER STAUB: I just wanted to weigh in on the on the question what does the registry do if the registrar is not sending the data? And that is indeed the typical problem that we see. I can give you one example: worldathletics.org used to be the privacy registration for quite some time. It recently changed. They say they put the previous name of the organization. World Athletics is the international federation of all the athletics organizations basically. A really big organization. They're in Monaco, of course. It's not maybe a standard jurisdiction, but still, they were just sent by the registrar as privacy. Who cares? We're not sending this. Do not want to take any risks.

But say, if we want to deal with that problem, we can do this in a positive manner by offering a way to prove who you are. And thanks to the existence of LEIs now, there's actually a very good way to do the proof because they can actually go and put their own domain name and actually prove that they have the domain name in their own DNS and associated with it with the LEI. It is not something impossible to do. The pointers used to prove control of a domain name, and match it against another record, that's been around for ages. That's not something new. We can do that. It is just a matter for us to kind of get together and

endorse a standard, so that not every registry has to develop its own procedures to do that. If we, as a group here, come up with a couple of procedures—I'm taking also what Marianne said. We have many procedures, which is kind of … If you standardize them, they become much more credible, and of course, much cheaper to actually apply. They don't have to be compulsory. Just optional. It really helps quite a bit.

ELENA PLEXIDA: Thank you. I might be a little radical here. But I think we're having the wrong discussion. What I mean by that, we are discussing what are we going to tell policymakers to help them implement NIS2. So are we going to go there and tell them implement the article about data duplication, avoid data duplication, as it means thin WHOIS or it means WHOIS? No, we shouldn't do that.

I think it is very, very fair to point to the multistakeholder existing policies and procedures, and also point at the same time at the uniqueness of the ccTLDs. In other words—and I think that was your point, if I'm not mistaken—there are things that are already there. And Amadeu I think made that point. What we should be telling to policymakers is this is a minimum set. Don't go into details. Besides, it's one thing for policymakers to put in the high-level legal obligation to collect data, the high-level legal obligation to give access to data and another thing to go into operational details such as these are the data sets you will collect and maybe different in 27 member states. This is the way, technically I mean, nitty gritty, that you're going to do the disclosure. That is what the multistakeholder model is tasked to do. The

community is here to make these [policies, the specifics. It is not] there to do laws. Laws belong to the policymakers. So again, the point I'm trying to make is I think it is fair to point to the multistakeholder model. They themselves are trying to recognize that there. And yes, Amadeu, I couldn't agree more. The addition that they respect these policies to the extent possible, it's killing me. What does it mean? You respect it or you don't. And the uniqueness and [inaudible] between the ccTLDs that need to be different because of the difference of all the countries. Yes, that's what we should be doing. At the same time, we should have a consistent message for sure. We're all in this together.

Pointing out what could be the bad effects of fragmentation, what could be the effects of maybe not adhering or not sticking to the commitment of the multi-stakeholder model. That's it.

Then it is a separate discussion, but still very pertinent. What are we doing here in this community to avoid, if you will, another NIS2 or something that will not be as high level as NIS2 that is [inaudible] trying to put their legal obligations but still not details. [We don't know about implementing laws.] Thanks.

NACHO AMADOZ: Thank you, Elena. Just a second before going to you, Dirk, and with a warning that we have ten minutes. There were some concerns before this session that were raised about us as the GeoTLD group calling for an ICANN policy to be developed in this regard. Okay, yeah, sure. No worries, we need to work within the multistakeholder model. We need to approach regulators with this threshold that doesn't go beyond what is in the law. And I think that this approach is where we are converging

on what we should be doing. But we are happy with any participation or anybody saying this is what we are afraid of and this is what we think we should put into what we say for this common message or not. So please, maybe not stand up today because we don't have any more time and I'm not taking any away from you. But let's keep the discussion going. Dirk?

DIRK KIRSCHENOWSKI: I just want to make clear that I don't complain about those registrars which send only redacted or proxy data because they might do the right things because we don't have a data transfer agreement with them. I rather should complain with those registrars which send us the data without any agreement. That's the short statement I want to make to clarify.

VOLKER GREIMANN: Okay, that button doesn't like me. I just wonder if this group is maybe not just too small, not the right group to discuss this. I mean, we're the ccTLD operators, some of us here, and the gTLD operators. But this is actually a discussion that has to be had by all contracted parties in the industry because it doesn't matter whether you're a GeoTLD, or generic TLD, or a closed generic or open generic or what have you for a TLD, you are going to face the same obligations in the different countries in Europe, where you're being sold.

So I think the first step that we should take is what is the baseline verification agreement that we already have in place? What are the current obligations that the multistakeholder model has come up with?

Because the multistakeholder model is being referenced by the lawmakers as a potential model. So what do we have in place? That's the verification requirements, the validation requirements that we have in the RAA, for example. There are various verification requirements that we might have from our contracts with ICANN and other forms. And then we have to look at are those enough or will they need tweaking or expanding upon? And if so, in what form? What will be seen as enough by most lawmakers? And from that we build basically a community model that we go out to sell or to propose as the solution that we have come up with as the multistakeholder model.

But we cannot start inventing the wheel afresh. We have to build upon what we already have, because that is what the multistakeholder model has come up with and that's what's being referenced. Thank you.

NACHO AMADOZ: Volker, I think that we can see that this session would absolutely agree with what you said. this is not a topic that is specific for geos. It concerns geos, so that's the reason why we thought we need to start talking about this. And we are very happy with all the interventions that are not specifically from the geo space. So yeah, absolutely agree. And we want this to be a conversation that includes absolutely everyone. I mean, it doesn't need to be led by us or doesn't need to converge into what we think is the perfect solution. No, no. We need to really start discussing about what we do in that approach and that includes everyone. Michael Palage, you had the word. Please go ahead. Two minutes.

MICHAEL PALAGE: 60 seconds on the clock. So I agree it needs to be more inclusive and I think we have to take into account the non-contracting parties because clearly the reason NIS2 happened was there were certain noncommercial parties that felt that the ICANN process was not working, and they decided to go to Brussels. So I agree with Volker. We need to have more people and when we, the multistakeholder model, go and communicate, it needs to be more than the people in this room. Thank you.

NACHO AMADOZ: Even less than 60 seconds, please.

[LORI SCHULMAN:] As a non-contracted party, I definitely want to plus-one that. I also hear were Volker is coming from and where Thomas is coming from. But that's exactly right. There were some open questions left here that those of us who are non-contracted parties feel was definitely left out of the discussion and purposefully. And there was a need for clarification from the government that created the questions. That government now is trying to create some answers because it is a directive and not a regulation itself. Yes. Now we have to go to 27 jurisdictions rather than getting an answer from the top but that's okay.

And I just want to make it really clear that there are issues here and agree that this was open so broad, it leaves a lot of room for interpretation. And those of us who have an interest on the non-contracted party side and have legitimate reasons for wanting data to be kept and accessed as a public policy consideration, we will also be

explaining to governments the importance of why we need certain data and why we need it accessible, and when and how.

So yeah, it's great to talk about what the contracted parties need, because you're affected by the law directly. But so are the non-contracted parties. And I just want to make that very clear in the room. It would be great if we could align on some values and align on some common messaging. I think that would be critical. Now, are the policies at ICANN the common message? Frankly, I'm not sure, in terms of what we believe we got and didn't get in the EPDP process. And I'm going to leave it there.

NACHO AMADOZ: Thank you very much. Elena?

ELENA PLEXIDA: 30 seconds to me, too. I completely get everything. I just want to say what I said before. It's one thing calling for clarification of legislation or calling for legal high-level things and another thing to call for operational things that then enter into what the multistakeholder model is supposed to be doing. There, it is a distinction that we have to have to keep in mind that all of us are here to protect the multi-stakeholder model. That's the beginning and then we do the business and everything [around.] Thanks.

NACHO AMADOZ: Wrap up is going to be super quick, too. And that is going to be that we of course need to keep talking and we are super happy to go anywhere,

get anyone's feedback, make it as expandable or expand the discussion as much as possible, so that we get to this common set of messages that we can all fall behind.

Thank you very much and we are closing this session.

UNIDENTIFIED FEMALE: We can end the recording. Thank you.

**[END OF TRANSCRIPTION]**