JOHANNESBURG – GDPR and its potential impact: looking for practical solutions
Tuesday, June 27, 2017 – 15:15 to 16:45 JNB
ICANN59 | Johannesburg, South Africa

UNIDENTIFIED MALE: This is GDPR and Its Potential Impact, ICANN 59, June 27th, 2017, from 3:15 to 4:45, in Ballroom 1.

CHERYL LANGDON-ORR: Good afternoon, ladies and gentlemen. We are a few minutes late in starting this session, but we will be starting in only a moment or so. So if you have dinner dates and organizations and gossip to continue, take it outside. If you'd like to join us for this session here, which is the GDPR (General Data Protection Regulation) discussion. And that is what we're aiming for, a discussion. My name is Cheryl Langdon-Orr. I'll do that again in a moment, when the room is settled. But I just wanted to let you all know that we will be starting in only a moment or two, as soon as all of our people are at the front of the room who need to be. We are aiming to finish on time.

Good afternoon, ladies and gentlemen. We are now starting our session this afternoon, which is the General Data Protection Regulation discussion. And I'm going to keep using that word, discussion. I'm going to use it now by asking those that are having one to either find a seat or step outside.

My name is Cheryl Langdon-Orr, and it's my honor and privilege to work with you all this afternoon, and a couple of presenters at the front behind me, to have an awareness-raising exercise. We are not going to come up with solutions. We're not going to be grappling for consensus. We are, however, hoping that we will find some clear shared understandings of what it is we need to deal with.

We're going to have three presenters. Their role is to take a topic each and in, preferable, 10 – she says, beggingly, but if they have to have it, 15; begrudging, that will be given – minutes, they're going to set the scene. And they're going to set the scene because what we want to do – and we recognize absolute expertise as well as opinion in this room. But we want to make sure everybody in this room has a basic set of understandings of the topic that we will then spend the majority of our time together talking about, to which we will be, as some of you who've been to some of our sessions in the past, will have experienced having two moderators with microphones.

We have the four quarters, as is usual in these forum lately. So if you find a staff runner – hold one up on. Number 4, thank you, number 4, in the corner. If you look at number 5 – who can I have five quarters? I've got five sectors, apparently. You catch the eye of one of these people. They catch our eye, and we make sure

the microphone comes to you. That will be where we hope we will be able to maximize our input and interaction.

To do that, we're going to ask that you keep your interventions on topic. And that means, let's look at the nexus between the GDPR and ICANN. Not all the other really interesting stuff, right? We'll get the, "Off topic, next speaker," if you go down those pathways. So keep them on topic. Keep the interventions short, sharp. If necessary, no more than three minutes, preferably two. And if we have time, we'll come back to you again. But we want to have maximum interaction in today's session.

So, now, of course my notes have closed because computers are handy like that. It doesn't matter. I don't really pay attention to them anyway.

We have the three panelists this afternoon. They're not panelists. They're going to be presenters. They're not going to be panelists. They're going to be presenters. We will take the time to have a couple of questions put up just to get some of your thought processes going, but you do not need to stick to those questions. So when we put those questions up, you don't need to be limited to it. It's just to give us something to get started with.

Let's have the next slide. And I hope in the next slide – well, yes, that's what we're talking about.

Next. We've moved into our first speaker's topic. And I'm going to hand over, and sit down, to Cathrin Bauer-Bulst. I'm not going to do who they are and what they are. They can tell about themselves if they want to. We are then going to move immediately to Becky Burr. And then after Becky, immediately to Theresa. So I won't be interrupting. They will be moving, stopping. I might say, "It's your turn." Then we all get to play, and that's the part we need to get to.

Over to you, Cathrin. Thank you.

CATHRIN BAUER-BULST: Thank you very much, Cheryl. Good afternoon, everyone. My name is Cathrin Bauer-Bulst. I am here today representing the European Commission, and more concretely, my colleagues from the Data Protection Unit who couldn't make it today and under whose control I speak today.

Now, as you know, in the EU, the European Commission has the authority to propose legislation. And so a long while ago, we proposed the European General Data Protection Regulation. And I have the pleasure today to take you through some of the very basic concepts of this directive, sort of an introductory course on the European data protection framework, if you so will, which will be upon us a little bit less than a year from now. On the 25th of May 2018, it enters into application.

Next slide, please.

So I first want to take you through some of the overarching aims of the GDPR, as we like to call it, and then go through some of the key concepts and the governance structure. On the overarching aims that are behind this framework, is that in the EU, we found that with the directive that was in place before, the framework for data protection was still quite fragmented. So now we have introduced, within means of regulation, which applies uniformly across the whole of the EU one single set of personal data protection rules.

This also creates one interlocutor and one interpretation, meaning that if you're a business that does business in more than one EU member state, you now have one data protection authority that is mainly responsible for you, and you don't have to contact several ones.

It also seeks to create a level playing field, in terms of the territorial scope. And I will come back to this in just one minute.

And the fourth main principle was that it's trying to cut red tape. So one important issue that is now changed, or that will change in May 2018, is that until now, you needed to proactively notify your data processing operations to your DPA. This will no longer be necessary under the GDPR, which takes more of a trust-based approach.

Next slide, please.

All right, this is missing the basic principles that were supposed to be shown. So you will just really have to pay attention, because the beautiful, colorful blocks outlining all the principles are missing. But I'll try and be very clear about them.

So the fundamental underlying principle in the EU is that there is a fundamental right to data protection. And that is laid down both in the European Charter of Fundamental Rights and in the treaty that governs the workings of the European Union. And this fundamental right now translates into specific rights for individuals. And now you really have to watch out that you catch all of them, since they're not visible.

The first invisible one is the right to be informed. So the data subject has a right to be informed in concise, transparent, intelligible, and easily accessible terms about what is happening with his or her personal data.

The second right is the right of access. So under the GDPR, individuals will have the right to obtain confirmation that their data is being processed. They will have the right to access the personal data that is processed about them and any other relevant supplementary information.

There is also a third right to rectification. So if the data is inaccurate or incomplete, individuals have a right to have it be rectified.

The fourth right has actually generated quite some waves already and has become known as the right to be forgotten. In the GDPR, it is taken up as the right to erasure. So this applies when the personal data is no longer necessary in relation to the original purpose for which it was collected or processed or when the individual withdraws consent.

There is also further rights on restricting the processing. So, for example, if an individual has raised concerns about the accuracy of the data that is stored about him or her, he or she has a right to ask the processor to restrict the processing of the data.

And there's also two further right that I want to take you through. The right to data portability, which allows individuals to basically obtain and take their personal data along with them to another service provider, which has to be provided in an easily downloadable format.

Oh, see, here are my beautiful blocks. So you can see. On the penultimate one already, so the last one is the right to object. In specific situations, individuals have the right the object entirely to specific types of processing, in particular when it relates to

direct marketing or the processing for purposes of scientific or historical research.

So I hope you've all had time to review them now. We're going to move on to the next slide, please.

All right. You've already heard me use a couple terms that deserve a little bit further explanation. I'm going to take you through some very basic definitions now.

The key concept is personal data. That's what this regulation is built on. And that is any information relating to an identified or identifiable natural person. So that means it's not necessarily just your name or any other information that might, on the face of it, already tell everybody who you are. It's also information that, together with other elements, might help people discover who you are. And that can be, for example, if I register my name as a domain name, it is automatically personal data. But also one very good example that was used yesterday was if I have an e-mail address that is ceo@citibank.com, then it's also very easy to discover who that person is. So that is also personal information, personal data.

And that also means that it's not very easy to just define categories up front. My earlier example of the domain name, if you have the domain name table.com, obviously, it's not personal data. But if you have the domain name

cathrinbauer.com, it's a different issue. So that means it's not always easy to even define categories of data that are always personal data or that never contain personal data.

A second very important concept is that of processing of data. And that is really up to your imagination. Processing is really anything that you do with the data. You collect it. You store it. You analyze it. You delete it. You forward it. You publish it. It's all processing. You even think about that data, it's processed.

And then a third important concept that I want to mention today is the geographic scope, because there has also been some confusion around that recently. So the GDPR does change the geographic scope, as compared to the directive, to create a more level playing field. So while the directive focused on data controls and processors that were established in the EU only, the geographic scope of the GDPR is slightly wider. And it also applies to controllers that are established outside the EU but that have data of persons in the EU and that have processing activities that relate to the offering of goods or services to data subjects in the EU, or that monitor the behavior or persons within the EU.

Now, of course, this raises some questions around how that is further defined. And the concept of the GDPR is that you have to target the EU market in some way. And for this, it's not sufficient

– just to provide a bit more detail on this – to have your website be accessible from the EU or to be using a language that is the language of your home territory but also happens to be the language of an EU member state. So indicators that are listed in the framework are the use of a language or a currency generally used in one or more member states, with the possibility of ordering goods or services in that language; or the specific mentioning of users that are in the EU.

Next slide, please.

All right, now turning to the three key actors in the GDPR, we have the controller, the processor, and the data subject. And to start from the top, so the controller is the entity that determines the purposes and means of the processing of personal data. So basically, who determines why a set of personal data is collected, what should happen with it, and in which way, shape, or form it is collected or processed. The processor is merely, sort of, the entity who executes those policies set by the controller, and that just performs the processing operation without making any choices him or herself about what the purposes and means in the processing should be. And then the data subject is, of course, the individual whose personal data is being processed. And here, I've specifically put the "natural person." So it's very important to remember that personal data can only ever apply to a natural person. So there's no such thing as a legal person

having personal data. The scope is uniquely limited to the natural person.

Moving along to the next slide, I just want to go through some of the principles that apply to processing. So one key principle is that the processing has to be lawful, fair, and transparent. What does it mean for the processing to be lawful? It means that it has to have a legal basis, as outlined in Article 6 of the regulation. I just want to mention a few of the most important ones.

The first one mentioned is consent. So there is a possibility to process data on the basis of consent given by the data subject. That consent must be freely given. So that means you cannot condition the delivery of your product or service on that consent being granted. It has to be detached from the provision of the product or service.

Now, of course, you may need certain personal data for the delivery of your product or service or for whatever other contract, so there's a number of other grounds that can apply. And here, most importantly, if you need the data for the execution of your contract, or for even entering into preparation for the contract, then you don't need the consent of the data subject.

Another legal basis that you can use is if you are under a legal obligation to process that data or if there are vital interests at

stake or if there are legitimate interests of the controller in processing that data, which requires a balancing with the interests of the data subject.

The second principle is that of purpose limitation. And that brings us back to a concept that already came up that's very important yesterday and that I just want to take one minute. I'm keeping, of course, in mind Cheryl's timeline. So purpose. I think the general concept behind the GDPR is that it requires everybody to ask, "Why are you processing personal data?" So you need to take a step back and think, "What is my purpose? What do I need this for?" And then only in relation to this can you assess whether or not it is appropriate to process that data. And the purpose has to be specific enough to enable you to actually make an accurate assessment of that. And purpose limitation is the first emanation of that principle. So you have to collect for specific, explicit, and legitimate purposes, and you cannot process the data in a manner that is incompatible with those purposes later on.

The third principle is that of data minimization. So the data has to be relevant and limited to what is necessary in relation to your purpose.

The data has to be accurate and, where necessary, kept up to date.

There is a storage limitation. So if you no longer need the data for the purposes that you originally collected it for, you have to delete it.

And you have to ensure the integrity and confidentiality of the data.

Next slide, please.

Yes, I just wanted to take one minute to review the governance structure of the GDPR, because I felt that there was some confusion around this. And that also explains my role here as the European Commission. So we're not in the practice of providing specific guidance on individual applications of the GDPR. That's not our role. So the architecture is actually as follows.

You have your national data protection authorities, which are your key go-to point. And they are the ones who can issue decisions, including on fines. So the GDPR actually foresees an [enforcant] regime, which I think is one of the parts that there's most awareness about in this community, so I'm not going to go into much detail on this. Only to say that there can be hefty fines for not complying with GDPR. And those are in the purview of the national data protection authorities. They can also provide advice on the application of the GDPR.

Those decisions can be reviewed by the national courts. And individuals can also apply to the national courts if they think that action should be taken in any way, shape, or form. And if there's questions of interpretation, the European Court of Justice is the court that will provide the final and definite interpretation of the GDPR.

The national data protection authorities come together in the European Data Protection Board, which very importantly has a consistency mechanism. So when there's differences in interpretation between different national data protection authorities, it is up to the European Data Protection Board to resolve those differences. And in that case, it can also issue a binding decision. It is the replacement of the Article 29 Working Party that a lot of you are familiar with already. And it can also provide guidelines and issue advice on the application of the GDPR and has already done so in preparation for its implementation.

Now, the European Data Protection Supervisor serves as the secretariat of this EDPB (European Data Protection Board), and also sits on it. The European Data Protection Supervisor is the entity that is responsible for supervising the processing of the European institutions subject to a totally different set of rules.

Just to make it very clear for everybody, we have the Board that is really the go-to point for all the international questions. And then we have the Data Protection Supervisor for the European institutions, which has the title of European Data Protection Supervisor.

And then I don't know whether the rest of you can still see the slide. So just to say that the European Commission is also in charge of implementing the rules and is the guardian of the treaties in this way. So it works with the member states to ensure that the data protection rules are correctly implemented.

And I think I'll stop here and turn it over to Cheryl. Thank you very much.

BECKY BURR: Thank you. I hope we have the slides I'm going to use. My name is Becky Burr. I am Neustar's chief privacy officer in my day job. I'm also a member of the Board. But today, I'm really here just to talk about how a chief privacy officer would go about figuring out what needs to be done, if anything, to come into compliance with the GDPR. And I'm going to put that in the context of ICANN and contracted parties.

Do we have my slides? I have them here if we don't, but it would be great if we could pull them up. Okay.

So contracted parties, ICANN establishes through contract, and the community establishes through policies, a lot of obligations that require contracted parties to collect information about registrants, about business relationships, transactional data, information when you apply for a new gTLD, information about your shareholders and chief executive officers.

So there are over 60 data elements that have been identified that are required either in ICANN contracts or policies that contracted parties must collect. Many of these – actually, all of which are potentially personal data. I just want to do a little riff on the personal data stuff.

When people come into my office and say, "I want to do something with data, but it's no problem because it's not PII," I say, "Go outside, and when you stop saying that word, you can come back in and talk to me." Because we talked about a legal person. So chiefprivacyofficer@team.neustar doesn't have a name in it, but anybody who wants to look on the Neustar website can figure out that I am Neustar's chief privacy officer. So unless I'm quite mistaken, that would be personal information under the GDPR.

So basically, when you look at that, depending on what the combination of data is, all of these 60-plus elements are potentially personally identifiable information. And there are

various obligations that go along with it. Registries and registrars have to retain it. Some of it has to be escrowed. Some of it has to be published under the various policies.

All of those things – collection, retention, escrow, publication – all of that is processing. Every single one of it. And one of the complexities is Cathrin put up a data controller decides what the purpose of collection and processing is, and a processor just carries it out. There are lots of ways in which sometimes we're processors and sometimes we're controllers. And there can be two controllers in any one situation. So it's not a straight line. So that's what we have to do. That's where we start from.

Next slide, please.

Under the GDPR, as Cathrin said, you have to have a lawful basis for processing personal data. Now, I'm going to skip all of the other things that say, "You have to tell people about the data you're collecting and what you're doing with it," and all of that. But I just want to, for this exercise, focus on what's the lawful basis for processing this personal information.

It's not exception that Cathrin referred to about contractual, to fulfill a contract. That means I have a contract with you, data subject, and in order to provide the service that you've asked for, I have to process your data. That's not what's going on here.

Typically, in the WHOIS context, we've relied on consent in a sort of opt-out fashion that basically says, "I'm going to give you a choice." You know you have a choice. You could do something, whatever. You proceed to register a domain name. You've made a choice.

Now, not actually very much of the substantive data protection law is changing from the directive, as implemented by all of the member states in Europe. But one thing is really changing, and that is the ability to rely on consent. As Cathrin says, it has to be unambiguous. It has to be freely given. It can't be a condition of providing a service. And there is a strong presumption for anything that involves automated or continuous processing, that it's not going to work.

So relying, as we have in the past, on consent for collecting and publishing this data is very hard. But the purpose that will work, and I think that we all have to turn to, is this legitimate basis. So to further a legitimate purpose of the user of that data, so long as that purpose is not outweighed by the privacy interests of the individual data subject, the person who the information is about.

So to even get to the point of figuring out how to do that balance, we have to collect that information. Now, even when you have that balance all worked out, you still have to make

sure that there are adequate safeguards in place. So that's something that we'll come back to.

Let's go to the next slide.

So the lawful basis – and this is sometimes referred to as a proportionality test – is there's a lawful basis for processing personal information if it's necessary to achieve the legitimate interests of the data processor, except where it's overridden by the privacy interests of the data subject. So as I, as a privacy officer for a registry, go through this, I'm going to be thinking about collecting the information that I need to put in front of my advisers, that I need to advise my clients, that I need to consult with data protection authorities on, to engage in that balance test.

Next slide.

So I just want to set this up in the order. First, in order to do that, in order to do that balance, first I'm going to say, "What data elements are out there? What are the data elements?" Remember, we talked about there are 60. So we have a list of 60 data elements that are collected. And then I'm going to say, "Who wants to use those data elements? What data elements do they want to use? And why do they want to use them?"

Once I have that all collected – and at this point, I haven't asked the question, "Is it legitimate?" And by the way, I also haven't asked the question, "Is it personal data?" But once I have that information collected, then, and only then, can I actually do the balancing test, the proportionality test, and say, "Okay, here's an interest. Let's assume it's legitimate. What are the privacy rights of the individual?" Because often, that's going to have some impact on whether the use is legitimate. And how do those balance?

And if they balance, then assuming I can find appropriate safeguards, then I'm going to feel like the GDPR will allow that processing to take place. But if they don't balance, if the answer is, "I make balloons, giant helium balloons. And outside of ICANN 60, I want to have giant helium balloons that have the personal information of every registrant that I don't like flying around out there." Then we'll have to talk about whether that's a legitimate use or not. Or if I'm a spammer and I want to data mine WHOIS data to spam everybody, then we'll talk about what's my privacy interests in not getting spammed. Also, what's the rule in ICANN. That is another piece of it.

But what I'm talking about is just what I need to have in place in order to have a sensible conversation about how to apply the test that says whether the use of the data that I am facilitating as either a controller or as a processor – I probably am both –

whether that works under the GDPR. So it's a kind of step-by-step thing.

Next slide.

So when I do this with my internal clients, what I try to do is put this as user stories, because ultimately, whatever we come up with is going to have to be built. And I've got to explain it to an engineer, who I have forbidden to contemplate whether something is personal information or not.

So I'm going to say, "Okay, here is one user's story. As a law enforcement officer, I need data elements 1 through 27, and 29 through 60, in order to identify persons engaged in DDoS attacks on the Internet." And I'm going to go through all of those purposes and have a complete list.

"As a network operator, I need data elements number 27 and 28 in order to figure out how to route something to someone or figure out if there is some kind of misconfiguration and understand who to talk to in that place. I'm going to get those things all lined up."

"As a registry, I need to collect this information in order to bill registrars and in order to report to ICANN, as I am required to do." A whole list of fairly detailed – what I want to do is collect all of the users out there, all of the purposes that they might have

for accessing this data, and then all of the data elements that they would need in order to accomplish the purpose that I've described.

I'm going to make it pretty granular, because when I go and talk to my lawyer or I go and talk to a data protection authority, I don't want to say, "As a law enforcement officer, I need all of the elements in order to catch bad guys," because the data protection officers will say, "I need to know a little bit more. Give me a little bit of detail."

And I think that you saw that if you read the responses that we got from the data protection authorities who were with us in Copenhagen in response to the RDS questions, those 19 questions. A lot of what they said, "Well, it sort of depends. We need a little more information. Who's using it? What are they using it for? What data are they using?"

So that is how I'm going to proceed. And I'm just trying to lay this out so… One of the things that I've said is, "Well, I'm a contracted party. I'm doing this." But you notice I'm talking about user stories. Well, I don't think I'm going to be excellent at thinking up all of the user stories that law enforcement might have or rights protection folks might have or people who are engaged in anti-abuse activities, the anti-malware and anti-phishing coalition, all those kind of things. So I'm going to want

to gather input from users so that I understand what their uses are, what the data elements they need are, and what the users' stories that go along with their case are.

I think I have one more slide, and it's just a picture that basically says, "Here's the matrix that I'm going to build." I'm going to say, "Here are a couple of the elements that ICANN requires us to collect and in some cases to escrow, and in other cases to publish. Here are the policies that do it. Now, let's get the purposes written down."

I'm done. I hope it was less than ten minutes.

CHERYL LANGDON-ORR: Hm. Theresa?

THERESA SWINEHART: Okay, I'll try to keep to the ten minutes desperately. Let me just briefly talk about what ICANN, as an organization, is undertaking. And I hope everybody had a chance to also see the blog that was put out prior to the meeting by both Akram and myself to help outline that. Since then, obviously, there's been some moving parts and quite a few discussions that have been occurring here. But clearly, we're dealing with a situation that's quite unique and that has a timeline to it. And so figuring out

how to move within that context with the community, as Becky had outlined.

And so in order to look at this, given the fluidity of the situation as well and the effect that the GDPR has on ICANN as an organization, we are taking at two-track approach. Well, sort of a three-track approach. We're looking at the implications of the GDPR on ICANN as an organization in relation to data that ICANN, as an organization, has. And that can also involve data that relates to our engagement with the community in the sense of travel support and other aspects of that. So that's a fundamental ICANN organizational standpoint, and that work is being undertaken.

And then the second part is the dialogue that Becky had also started talking about. And that relates to the engagement with the contracted parties and looking at what the current situation is in relation to compliance and the potential implications of the GDPR overall in relation to that.

To help us manage some of these activities, under Göran's leadership, we have an internal task force that helps us just track where we are with these different moving parts that are under existence, and then on the engagement part, which I'll touch upon briefly.

So in relationship to the dialogue with the contracted parties, I know the GDD team and many of you have been involved in some preliminary discussions that had occurred both in Copenhagen, at the ICANN meeting, and then more recently at the GDD Summit that was held in Madrid. And building on that, we really need to understand what the implications are of the current situation.

And I want to be quite clear. This has nothing to do with some of the policy development work that's underway, the work of the great RDS group that met yesterday and the dialogue of what is happening in the future. This is purely taking a snapshot of the current situation that's underway.

And part of this is for us to be able to understand the context of what we need for a legal review and for the engagement with the DPAs. And that's really to identify the relevant registration data elements that the registrars are required to collect and maintain, identify the purposes of these registration data elements, and understand which data elements are required for the identified purpose.

So in order to do this and to engage with everybody who has different uses and purposes for the data elements, we want to work with the community around this, to help us identify the three key elements that we need to be looking at. And for that

purpose, we're engaging also with a small group. I know the SO and AC leadership may have been reached out to, to help us inform what the purposes are around this so that we're not missing anything with regards to that, how to fill in a matrix that says, "This is what law enforcement needs it for. This is what intellectual property community needs it for," so we have clarity around that.

And again, this exercise is not intended to assess the legitimacy of the uses or purposes, but just to gather a comprehensive list around it. And the output of this group would be published to get additional inputs. And obviously, the work of this group would be done in a transparent way.

Obviously, the cadence of the timeline is quite important. I think we saw the timeline that was put up at the beginning. So making sure that we work concretely and quickly around this related work. And then to make sure that we get out there for the opportunities to engage with the data protection officials around that.

Let me touch briefly on the engagement side of this. Clearly, there's a lot of conversations happening. ICANN, as an organization, needs to make sure that we're working within our mission and scope as an organization, not exceeding that in any way. So we are engaging in different outreach events and

engagement opportunities, whether within the European realm or in other jurisdictions, where there's dialogues around data protection, issues around that and keeping track of what's evolving in that space so that we can help be proactive also in the context of some of the dialogues that are occurring and that effect either ICANN organization specifically to our operations or in the relationship to the contracting parties.

So I'm happy to take any questions around that or have the GDD team elaborate any more on any specifics, but that's an outline of where we are now. Again, it's very fluid. We will keep everybody apprised of the fluidity and what we're trying to facilitate here. Thank you.

CHERYL LANGDON-ORR: Thanks, Theresa. And thanks to both Becky and Cathrin, as well. Now we want to start turning to you. But if we can have our slide with our little primer questions which, as I say, we don't need to stick to. But if none of you can't think of anything to say, these might get you started. Although looking at some of the luminaries I see around the room, I'll be very surprised if we can't [really]. And we have someone who's in from remote. But let me tell you, just before we go, I will give preference to remote input at all stages, where possible.

Go ahead, please.

UNIDENTIFIED FEMALE: Question from a remote participant. "What is the procedure of identification of the relevant EU DPA in case when the company is based outside of the EU and provides services to EU citizens of few EU countries?

BECKY BURR: I'll just paraphrase the question. The question is, "I'm a registry. I'm based in the united states. I know that maybe I don't have a physical office in Europe, but I do have registrars in Europe. They send me data. What data protection authority do I work with?"

CATHRIN BAUER-BULST: Right. So I'm speaking under the control of my data protection colleagues here, but my understanding – and I'm happy for any input from other experts in the room – it depends on where the gravity of your presence in the European Union is. So if you don't have a physical establishment, then you are expected to nominate a contact point in Europe in a member state of your choice, to my understanding. And then that person would be the contact point for the local data protection authority. But maybe also [Olivo] can weigh in on this.

He was just saying that I was correct with my educated guess, so thank you.

CHERYL LANGDON-ORR: Great. Okay. So we have got two moderators. They will move to you. I see 3 up first, [Peter], and then, [Oliver], if we can go to 4 next for you. Thank you very much. And, please, just make yourself known, and these people will come to you.

Go ahead.

[TED HARDIE]: [Ted Hardie] with a question for Theresa, a scoped question about what the taskforce at ICANN is looking at. Obviously, there are some registries at ICANN that are maintained by IANA, which are specified by the IETF, which might include contact information or other things which might be the subject of these regulations.

Is your taskforce looking at those as well, or do we need to set in motion a different process for those?

THERESA SWINEHART: So as part of our internal, we would be looking at anything that we need to deal with. But if we have question, then we would also reach out to any of the affected parties.

UNIDENTIFIED MALE: Okay, let me go first to the middle of the room. [Peter]?

[FREDERICK GREIBAN]: For the record, [Frederick Greiban] speaking, Key-Systems, European registrar. One thing that becomes increasingly clear, looking at the impact of GDPR, is that WHOIS as we know it today is already a thing of the past, or should be a thing of the past, because the GDPR is already in effect. And by publishing information for everyone to use without purpose, or without legitimate purpose, is already violating. There's just no enforcement element yet. So we are essentially already violating the laws and the regulations.

So while we are willing to work with ICANN to resolve this issue, we are very aware that we have a problem already and we need a solution for that. And that means getting rid of free public WHOIS as soon as possible, at least for natural persons in Europe.

CHERYL LANGDON-ORR: Becky just wants to reply then. It's over to you, Becky.

[FREDERICK GREIBAN]: Okay, thank you.

BECKY BURR: So I think that we're going to probably hear a lot of expressions along those lines. I think that the exercise that Theresa outlined is deliberately designed to help get to a solution, and it is deliberately designed to place the information – collect the information, put it in front of the data protection authorities, get answers and input from the data protection authorities and law enforcement.

Everybody gets to have their own view right now about what the data protection authorities are going to say. But one of the rules that we hope that you will indulge us in is we're not going to have that argument as we go through the exercise, because otherwise we will never get there. Let's try to have a judgement-free exercise, where we really get the data in front of the data protection authorities, and everybody gets to hear what they have to say.

UNIDENTIFIED MALE: Okay, I can add to that, because registries exist in different shapes and formats. Pretty much is going to determine how you are set up as a registry also. And whether or not you have a contractual relation with your registrants and whether that purpose thing that you mentioned is also applicable to a WHOIS service that you're offering. But let me take a question here.

[BIETRICH PIEN]: Shall I use this? Thank you very much. I tried to respond to the constraint posed upon us and tried to be brief, but I thought it would be maybe not a question, but some comments coming from data protection authorities side and the stance that they have and that, and maybe to briefly convey their message to the distinguished audience here.

Let me start by answering the question. I don't think it will change, really. The entry into force of the GDPR, the fact that data protection authorities all over Europe, and to some extent outside of Europe, keep repeating that for 15 years in some communications in letters that there are issues when it comes to ICANN Bylaws compliance to data protection legislation, and in a broader sense in data protection standards.

Practically, it touches upon issues with private information of the data subject, [proportionality] of WHOIS data, the publication of WHOIS data, third-party access, and the accountability for processing data. It has been repeated several times. And the Council of Europe, under the mandate of the Committee of Ministers, facilitated, as you may know, a meeting between data protection community and ICANN community, with the participation of Göran, [special operator] on rights and privacy, European Data Protection Supervisor, the co-Chair of Article 29 Working Party, the DP of Interpol, Chair of the Data

Protection Committee, and the Concert of Europe director [inaudible] Information Society.

And this was basically, to cut the long story short, to say that, "We are here. There are issues. But let's work it out together." And I think I'm going to finish it very briefly. I think we are going into the right direction, because we already sense some move and some developments. But whether if it's enough or not, that community will decide.

Of course, for me, it would be very important to convey the message I have been asked. So the message from this distinguished person and participants of the privacy day in ICANN 58 would be that ICANN should put in place its own [inaudible] structure privacy policy to be in compliance with international privacy standards. And at that, to even prevent if assessment should be carried out of the impact of processing of personal data on the rise of the data subjects –

CHERYL LANGDON-ORR: Thank you very much.

[BIETRICH PIEN]: [inaudible] referring to –

CHERYL LANGDON-ORR: Sorry, I will… Okay, come on. And we will publish that. Please, if you can give that to our staff down the front, we will make sure that becomes part of the transcript. Could I ask you to identify yourself? My name is Cheryl Langdon-Orr, and we all need to identify ourselves every time we take the microphone.

[BIETRICH PIEN]: Yeah, [Bietrich M. Pien], Data Collection Unit of Council of Europe.

CHERYL LANGDON-ORR: Thank you very much. Now, we have someone on remote, but I know that [Olivo] has someone over there. So let's go to you first, then we'll go to remote, and then we need a microphone down in the front.

[OLIVO]: We have two questions on this side of the room. One is from [Erica Arman], and the other question after that will be four rows behind you.

[ERICA ARMAN]: Actually, I don't have a question, but I have a comment. I would recommend to you – and Theresa in particular and Becky – when you do the evaluation for this community, you don't assume

that, despite having European [right] common regulation that everything will apply in the same way to the different member states. There's still some grey areas. So it depends on the topics you are looking into. And I think this is advisable because companies will be headquartered in different European countries. So it is definitely advisable, beside waiting for the common approach, you are looking forward to look at the same time what kind of response you get either from a local law firm or from a chamber you are working with or colleagues you are working with in a similar environment. Just keep this in mind.

[OLIVO]: Thank you. There was one person before you.

AYDEN FERDELINE: Ayden Ferdeline, from the Noncommercial Stakeholders Group. I had one question that might be best placed for Theresa to respond to. In relation to the taskforce that you mentioned ICANN had established to discuss the implications of the GDPR, can you please tell me about the composition of the group? Who will be working on registrant issues? And also, whether or not transcripts from the taskforce will be released and made public. Thank you.

THERESA SWINEHART: You're referring to the group that I described that's going to help put together the matrix? Yes, that'll function in a transparent manner. It'll be a small group, but we'll make sure that it functions in a transparent manner around that. And we'll make sure that those processes are in place.

So the composition we have, it's members of the contracted party group. And then we have reached out to the ccNSO to ask either the leadership or to identify somebody, a designee. So as soon as we have that composition, we can get that to you. It's just been very fluid and very rapidly moving.

CHERYL LANGDON-ORR: If I might, Becky just wanted to respond to what [Erica] asked, so we'll take that first.

BECKY BURR: So I just want to agree with [Erica] that of course everybody is going to have to understand their own situation and understand what their roles are, that the data protection authority that they are responding to is going to imply. But we are going to make an effort to get some collective input from the Data Protection Commissioners to minimize that to the extent possible.

CHERYL LANGDON-ORR: I believe we're staying in this corner of the room. And then, so we all know, we're going to come down the front. Then we're going to go over to station 3, and you can manage this area here.

ANDREI KOLESNIKOV: Andre Kolesnikov, ALAC. Just a little complaint. Now we approach GDPR, which will happen in year of '18 right? But the problem with the registrations are not new. There are different regulations, different countries, which require certain setup for the domain name. For example, in Russia, we have to localize the data. For example, any registration with .com or the Russian [inaudible] may bring the registrar into the very twilight position because the data must be located in Russia. Okay?

There's many things prior to GDPR which were known to ICANN. And my question is why it took so long to face the problems. Very simple question.

CHERYL LANGDON-ORR: And now I'm leaning forward to give you an answer. Maybe they'll come up with something a little later one, but thank you for the question.

We're coming to you, [Peter].

BENEDICTO FONSECA: My name is Benedicto Fonseca, from the Brazilian government for the record. I'd like to thank for the presentations, especially the one made by Cathrin, in which you have mentioned the different elements that are included in the right to personal data protection. I think most of these, with some nuances, are present in the various jurisdictions and should not be matters so much confusion. Right to be informed, to access, [notification], etc. But the right to be forgotten, or the right to erasure, is something very particular to the European context.

So my question is, in the context of the operation of ICANN, is it something that has relevance? And in that case, has it been addressed? Maybe Theresa, that will also be, yes, addressed to you, that part of the question. Through your internal discussions within ICANN, has this been a matter of particular concern? And how has been the experience in trying to implement and to adjust that part of the GDPR to the operations of ICANN? Thank you.

CHERYL LANGDON-ORR: Go ahead, Theresa.

THERESA SWINEHART: I think, as I mentioned, we are in the process of undertaking this. So I should be able to have some more information for you in the near future.

CHERYL LANGDON-ORR: Cathrin?

CATHRIN BAUER-BULST: Just to clarify, so this right is also not an absolute right. It applies in certain circumstances, for example, when the personal data is no longer necessary in relation to the purpose. But there is also the situation where the individual might object to the processing, but there is an overriding legitimate interest for continuing the processing. So it is provided within limits, and the law in and of itself doesn't set this out as an absolute right. And I think that's very important to remember. Thank you.

CHERYL LANGDON-ORR: I think I saw [Thomas's] hand up some time ago, and number 4 is not next, even if I was going to number 4. So let's keep the flow going.

[THOMAS LECAT]: Thanks very much, [Peter]. [Thomas Lecat] for the record. I'm representing [Acor] Internet Industry Association which has, in

its membership, more than 1,000 members from more than 60 countries, most of which are facing the GDPR challenge. And I've been quite involved and engaged in the discussions with ICANN. And I think there are some conspiracy theories in the making.

And at least my expectation from these discussions is that we would try to work on the contractual compliance aspect of things in order to avoid the parties to be sanctioned. And therefore, you should not expect anything to come out of this that goes beyond the bare minimum. And therefore, this is a contractual issue that needs to be worked on, but the challenge for the companies is far broader. You can not only expect from these discussions something to be the output that is limited to the contractual interface to ICANN. Your operations as registries or registrars encompass far more to do with personal data. And you should be starting to work on that rather sooner than later, because it's a big effort

And for those who are outside the European Union, operate out from other countries, you might say, "Why should I bother?" You actually do need to have a representative if your dealings with the EU are not just random. You know, there are a few exceptions. You should look into the regulation. But if you fail to put in place a representative, you might be facing up to 10 million euros in fines.

So don't take this lightly. This needs to be a joint exercise. And I think we should strive to working all together on this in a collaborative fashion. I see that this is starting in a collaborative fashion. It's early days, but I do hope that we're going to come up with something meaningful that everyone can subscribe to without mission creeping into other areas of the GDPR in a timely fashion so that everyone is prevented from being sanctioned. Thank you.

CHERYL LANGDON-ORR: Number 3?

ELLIOT NOSS: Elliot Noss, from Tucows. Cathrin, my question is for you, if I could. I want to check my interpretation of one your slides, the slide that laid out the enforcement mechanisms. As I saw that slide, we would have enforcement against us from the individual national DPRs, which would then be enforced or not by national courts, and then by the European Court of Justice if there were still issues.

So my first bit is, is that correct?

CATHRIN BAUER-BULST: Yes, that is correct. And the European Court of Justice would not step in as part of the enforcement mechanism, per se, but rather just if there were questions of interpretation of the GDPR. So if there was an [unclarity] around a provision, there's something called a preliminary reference procedure by which the national court can ask for a definitive interpretation of the GDPR.

ELLIOT NOSS: That's great. So I interpret that to say that there is no mechanism for a uniform interpretation. And we, as the governed, we certainly have registrants in every European state. We, as the governed, must assume that that will be interpreted on a national basis, it has every likelihood of being uneven, and that there is no mechanism for uniform enforcement, correct?

CATHRIN BAUER-BULST: That is incorrect. I'm very glad that, under Cheryl's strict regime, I now have two additional minutes to respond to this specifically.

ELLIOT NOSS: And, Cheryl, this is on her time, not mine, right?

CHERYL LANGDON-ORR: Absolutely.

BECKY BURR: If I might just add one thing?

CATHRIN BAUER-BULST: Sure.

BECKY BURR: There's a fact you need to know. I'm looking at their website. They have an establishment in Germany and the Netherlands. And that might help you answer the question.

ELLIOT NOSS: And Spain and a couple others.

CATHRIN BAUER-BULST: Right. So there's something called the consistency mechanism. And that is what the European Data Protection Board is in charge of. So if there are questions on the implementation of the GDPR, then the European Data Protection Board can help. And then there is also a mechanism for the cooperation between the national DPAs (data protection authorities) so that one of them can take the lead in a given issue. If the center of gravity is with that member state and then that DPA will coordinate with the other DPAs to make sure that it is giving you one and the same interpretation across your different establishments.

So really, the GDPR has thought of the situation of what happens if you're active in multiple jurisdictions, and I think it has solved it quite well. So I don't want to go into the details here, but there are multiple layers of mechanisms in place to make sure that somebody who is active in several member states is not exposed to differing interpretations of the GDPR.

ELLIOT NOSS: Great. Then last question, what would you expect – and I understand this is just in broad outline – the timing to be from the time an enforcement is filed through its working through a national court system? And sort of collateral to that, if there was an enforcement, would the violation be – would be forced to take it down the time of an enforcement mechanism? Or would it stay up during that mechanism?

CATHRIN BAUER-BULST: Right, so I'm going to give you a legal answer. It depends. It depends which jurisdiction you're in. It depends how obvious your offence has been. It depends what…

ELLIOT NOSS: Sure. Safe to say years on the light side?

CATHRIN BAUER-BULST: It depends. It could be much quicker.

ELLIOT NOSS: And it could be much longer?

CATHRIN BAUER-BULST: It could also be much longer, yes.

ELLIOT NOSS: Thank you.

CHERYL LANGDON-ORR: Thank you. Now, let me just make sure we've got the running order right. Who have you got?

UNIDENTIFIED MALE: Could we please go to the gentleman on my left, because he raised his hand?

CHERYL LANGDON-ORR: Okay. And then after that, we have the lady in red and station 4.

UNIDENTIFIED MALE: Okay, good. Over to you, sir.

[HALVUS AROSLEY]: Thank you. I am speaking in personal capacity. I have three small questions to Cathrin. What is your expectations of this European simplified framework? What is the next step? And second question is that you mentioned some conditions, such as lawfulness, fairness, transparency, purpose, accuracy, minimization, and so on, so forth. What are the modalities based on these that, if they are not respected, and if they are respected, and the abuse of that? And third thing is how treat the issue with respect to the national jurisdiction of the countries in which in future this may be applied? Thank you.

CATHRIN BAUER-BULST: I'm not sure I have an answer to the first question. I mean, I'm not sure what you mean. Do you mean, what is my expectation of what the GDPR will bring?

[HALVUS AROSLEY]: Yes, the expectations of European community [inaudible] or whatever from presentation? Do you want the community taking it into account, consider it, note it, further pursue it? This is expectations of the presentation. Thank you.

CATHRIN BAUER-BULST: Well, the expectation of this presentation here was simply to not just leave the community with awareness, but possibly with a

little bit more knowledge on what is actually coming and that a lot of it is not a revolution, but really an evolution of what has come before. So that was my personal hope for this session. It's for you to judge whether that has worked out.

But in terms of the factors and how those will be applied, so that will be for the data protection authorities – and there can be multiple ones in a given country – to enforce. And the GDPR doesn't really set any rules on in which order those are looked at our how a DPA should go about its work. It's independent authority, and it's up to the choice of the DPA what priorities it sets for itself. But the GDPR does, in the fines categories and in terms of the different mechanisms it has for reacting to a violation of the GDPR, it does differentiate between specific violations of the GDPR and categorizes some of them as more severe than others. I don't want to go into the details. I would invite you to look at the fascinating GDPR, all 88 pages of which I went through again yesterday. So I would just leave it at that for now.

And I'm afraid I didn't catch your third question.

CHERYL LANGDON-ORR: [Halvus], you have time to reiterate your third question.

[HALVUS AROSLEY]: The third question is are there any possible or potential conflict with the national jurisdictions of the countries in which this data is collected, maintained, or used? Thank you.

CATHRIN BAUER-BULST: Right. So there could be situations where the data is processed in a [third] state and is still subject to the GDPR, where there might be legal obligations that conflict with the GDPR. I mean, that's inevitable with any law. There can be conflicts of laws. And then one needs to find a way to resolve these conflicts. But I imagine that data protection authorities will also take into account conflicting obligations. And there is a specific reason – actually, what's it called – a specific justification for processing of data under the GDPR, for example, if you're under a legal obligation, to process the data. So that should reduce the conflicts.

CHERYL LANGDON-ORR: No, I'm not saying to do that now. I was saying you've just got to get that lady lined up. Not right yet. Not yet. Back on the starting block. Back on the starting block. No. No, no, no.

I am going to go you, because you have been so incredibly patient. And, yes, I know you're patient, number 3, as well. But

we do have a remote participant, so they will be next. Over to you.

KIRAN MALANCHARUVIL: Thank, Cheryl. Kiran Malancharuvil, from MarkMonitor, for the record, although I did like "lady in red," so you can say that too. A comment and then a clarifying question, please, for Theresa.

It seems to me that it's very, very important that, as a community, we look at what's been done in the past to extrapolate from the current WHOIS system what the purposes are for accessing WHOIS currently. I'm not talking about the inquiry that's happening within the RDS PDP. I'm not debating whether or not they're legitimate, illegitimate, whatever. But just an analysis of what is the current purpose of WHOIS data collection and access in order to see – because it sounds like there is a way to apply the GDPR uniformly. We need to look at what those purposes are and see how the GDPR affects each of them as a way to sort of give us guidance and hope as a community, rather than us having to go through these conflicts procedure, creating blanket exemptions for all purposes, etc.

It seems that there is a much more elegant way to address some of the problems the GDPR is presenting for our community. It sounds like maybe what Theresa is proposing is a good place in which we can do this, this sort of conversation. However, a

clarifying question, because you said the ccNSO and the contracted parties. And what I heard in today's open meeting with the CSG (Commercial Stakeholder Group), of which I am a member of the IPC, although I am speaking on behalf of MarkMonitor at this time, is that the CSG would also be included in that conversation.

So can we get you on the record then to correct your statement that it was ccNSO and contracted parties only? Thank you, Theresa.

THERESA SWINEHART: Yes. Yes, absolutely. In order not to go through all the acronyms, yes, absolutely. We've reached out to SSAC, ccNSO, CSG. And I understand that CSG is divided into three different parts. So appreciating that, looking forward to hearing back on that.

KIRAN MALANCHARUVIL: IPC, BC, and ISPC.

BECKY BURR: I think we failed to reach out yet to the ISPCP, but if they're dying to get in on it.

THERESA SWINEHART: The main point is that we have the relevant parties there to help populate this. And then also, we would anticipate that they might be going back to some of their folks to get some help on that. So really, the main purpose is to make sure we have the folks there to populate. And if I haven't read off all the acronyms, I'm terribly sorry. Let me know which ones I haven't, and I'll make sure to get back to those.

CHERYL LANGDON-ORR: Remote, please.

UNIDENTIFIED FEMALE: So a question from Michael Palage. "While ICANN should be applauded for tackling this GDPR issue, will the ICANN taskforce only look at GDPR or all international privacy laws?

BECKY BURR: We think that by looking at GDPR first, because it's the first on the horizon, but it clearly is not the only one. There are data localization laws that we absolutely know about, and there are new regulations, although the enforcement is not coming up quite as quickly. So hopefully we'll get a way to deal with these problems, but let us take on the GDPR first, please.

CHERYL LANGDON-ORR: We'll take it in relatively bite-sized pieces. I'm currently going with number 4. Then I'm going with number 3. Then I'm going with number 6. And then I'm coming down the front again.

Go ahead, number 4.

[FREDERICK GREIBAN]: Hello, [Frederick Greiban] again, Key-Systems. I am a big fan of not duplicating work. And a lot of research has already been done by ccTLDs in Europe that have already adapted different standards to their own display of private data. Some gTLDs that are based in Europe have already made changes to their WHOIS outputs. If you look, for example, at [.tel], [.cat], or even .amsterdam, who has applied blanket WHOIS privacy to all registrations in their TLD. Those are all solutions that are already in place.

Could registrars and registries be offered those, the same exemptions that exist from their current contracts that are already granted to other registries and registrars or that other registries and registrars not under the ICANN mantle, for example, ccTLDs have already applied for themselves?

BECKY BURR: I'm not ICANN's lawyer, so I'm not going to answer that question about… I mean, I think whether those specific exemptions will

apply. I will just say, we will take input from all of the sources that are available out there. There is some work that has been done as part of the Experts Working Group. There is work that has been done as part of the RDS PDP. All of that stuff is going to be input, and we do have a commitment, in order to move this work along, to be neutral and nonjudgmental. But all inputs are welcome.

CHERYL LANGDON-ORR: Okay, we're going to go to number 3 next. Then I'm taking a remote. Then I'm going to number 6. You've only slipped slightly because of the remote. Fear not. Then we're coming down the front.

Over to you, number 3.

STEPHANIE PERRIN: Wonderful. Stephanie Perrin, Non-Commercial Users Constituency. Kiran Malancharuvil actually came close to the question I was asking.

ICANN does have a rather large dependent industry of information services that has been gathering up WHOIS data over the years. On this taskforce, are you treating them as just another business? Because arguably, they're in possession of data that might be considered to be illegally obtained, because

ICANN, as the [daily] commissioners have pointed out, has not been in compliance for many years. So I'm just wondering, does ICANN, as an organization, consider them to be just another stakeholder or on a parallel track with the contracted parties?

And then my other question is, in terms of the access that is given to data that is held by the registrars, a lot of that, the protections are constitutional, not from data protection. But they are kind of contiguous. Will you be looking at that at the same time? Because it does have an impact on lawful access and, indeed, the cybercrime-fighting business. Thanks.

BECKY BURR: So no one up here is ICANN's lawyer, and so a huge number of those questions, I'm not even going to attempt to answer. The group that Theresa was talking about that was looking at the data elements that contracted parties are required to collect, escrow, and, in some subsets, publish through contracts and policies of ICANN.

CHERYL LANGDON-ORR: Remote?

UNIDENTIFIED FEMALE: There's a question from Michele Neylon. "When will ICANN appoint a data privacy officer?"

CHERYL LANGDON-ORR: No one's going to answer that, but I think by the acclimation in the room, a number of people think it's a darn good idea. Oh, hang on, somebody is going to answer it. Please.

GÖRAN MARBY: We have one.

CHERYL LANGDON-ORR: Follow-up from Michele?

GÖRAN MARBY: But could I raise something important, just for the record? We're talking about ICANN.

UNIDENTIFIED FEMALE: State your name.

GÖRAN MARBY: Sorry. Sorry. And I speak in a personal capacity. My name is Göran Marby. I'm the President and CEO of the ICANN organization.

The person we appointed is someone which works with the ICANN organization's information. So that's what we're doing. And we're doing this most because we think we actually think we need it, and the other reason is there are many countries around the world that has that function as a part of – for legal reasons. If I actually would remember her name right now, I would say that to you, but I can't. Thank you very much.

CHERYL LANGDON-ORR: Thank you very much. Now, we do have another remote participant [inaudible] that needs to be made now? No, it's the answer. Over to 6.

[JOHANNES LOCKSIN]: This is [Johannes Locksin], talking from [Surnet], a small registrar in Germany. I also work for Rotary International, where data is stored all in the US, from all members, centrally in Evanston in the US. And we decided to go the hard way. And the recommendation is to say, yes, we need written consent. And I would like you to address this, that if we have written consent and if we know our customers, we can ask them for consent, that we can go on with our business and even have a WHOIS service and whatever.

CHERYL LANGDON-ORR: Is Cathrin picking that up? Who's picking that up. Cathrin?

CATHRIN BAUER-BULST: Well, again, I'm not giving interpretations of the WHOIS. But of course, consent – interpretation of the GDPR and how it applies to the WHOIS, but of course, consent is one of the legitimate reasons under Article 6 of the GDPR. So I can repeat what I said before, and it needs to be freely given.

CHERYL LANGDON-ORR: And we're down the front now.

[DELILA MONET]: [Delila Monet], from the French government. I would like to know if there is any link between the GDPR, the Privacy Shield, and the activities of ICANN. Thank you.

CHERYL LANGDON-ORR: Go ahead, Becky.

BECKY BURR: So I think I mentioned that even where there's a lawful basis for processing, you have to take certain safeguards into account. So certifying your participation, your adherence to the Privacy Shield principles is the kind of safeguard that might be a

requirement. I don't know about other registries, but Neustar has certified its compliance to the Privacy Shield.

CATHRIN BAUER-BULST: Yeah, just to briefly explain, so the Privacy Shield responds to a specific provision under the data protection rules for international transfers of data. So if you're taking data outside of the EU, there's a set of rules that applies if a third country has been found to be adequate, and that adequacy is done by means of adequacy decision by the Commission. And one of the specific forms of an adequacy decision is the Privacy Shield, which applies to data transfers to the US and, therefore, is relevant to all of you who are regularly transferring data out of the EU and into the US. So that's definitely something to look at, not just for ICANN. Thank you.

CHERYL LANGDON-ORR: Over to station 3.

[AMADO ABRIL]: My name is [Amado Abril]. I am data subject, data controller, data processor, data victim, and a lot of other things, being a registrant, working for a registrar and a registry that's also an [inaudible] provider for ICANN. And I hate complaining all the time, but you do not allow me to do anything else.

We pretend. Let's talk frankly and live for once. We seem to discover now that there is data protection revelations in the [well]. The first ICANN meeting where data protection authority was present to discuss this with was in Rome, which was late February 2004. Since then, we have faced not just indifference, but let me put that way, overt and very strong hostility from ICANN staff to advance in any way.

Don't take that personally, Theresa. I wish you very good luck. I trust you. I like you. If there wasn't that many people here, I would even tell that I love you. But I won't, because I am very shy. So you will do a great job.

But the history tends to lead me to believe that in Abu Dhabi, we will say something about the 60 points. And I don't know, in Barcelona, October 2018, we'll seem to have missed all the deadlines. We don't need the discussion. We need solutions, quite frankly.

And, Becky, I beg your pardon. Once again, I am happy that now that Neustar, Tucows, and various are now affected, we can discuss about it. But regarding the 60 points, for the purpose of collection, well, we know what's it, even for possessing. The real question here are the transfers and the publication and other users who are not the pure registration chain. The real issue is publication.

And as somebody else – I think it was [Roger] – has said, we are in a very difficult situation ourselves. We are managing registries that have one exemption, but we are not allowed by ICANN to have the same for the others in the same jurisdiction, and that the protection [inaudible] is starting to get nervous. But ICANN condition forgetting the exemption are impossible.

So last question for Theresa, at very least, will you have a fund to pay for the fines, including the reputation damages?

CHERYL LANGDON-ORR: All right, I think we'll just take that as a question on notice. Thank you very much. We have very few minutes left. We have two remote participants, and I have at least [Thomas]. I think I'm going to close the line at that.

Let's go with remote.

UNIDENTIFIED FEMALE: The first question is from Maxim Alzoba. "Does ICANN have a backup plan to prevent escrow operators to cancel all escrow (registry and registrar) contracts to avoid fines?

BECKY BURR: So we are going to be looking at part of this at the escrow requirements. That's definitely a data processing activity, and

we will be looking at both the balance and whether there needs to be more safeguards in place.

CHERYL LANGDON-ORR: Next?

UNIDENTIFIED FEMALE: Next question, by Christopher Wilkinson, "How should an individual registrant proceed to ascertain which external entities have had access to our registration data? When, and for what purpose?"

CHERYL LANGDON-ORR: We're going to take that on notice, and we'll ask for some clarification. If he could type that into the chat, time is against us, and I'm not seeing light globes above anyone's head.

I do have [Thomas]. Do you mind waiting until last and letting number 5 go ahead? Please, go ahead.

ELIZABETH FINBERG: Hi, Liz Finberg, Public Interest Registry. I have a question. I'm not sure you'll have the answer, but it concerns the issue of consent. And so as I understand, conditioning service on consent is not actual consent. It's considered not to be freely given. However, my question is, how, if at all, does the availability of privacy

proxy services influence the issue of consent? Does the European Commission have a view on that?

CATHERIN BAUER-BULST: I'm afraid I don't have a view on that. Just to clarify, so consent is one way of justifying the processing of data. But of course, if you need the information to be able to fulfill your contract, then you have another legitimate purpose for processing the data. Just to clarify that.

CHERYL LANGDON-ORR: Thank you very much. And we will take any other questions in chat as on notice. I'm finishing with [Thomas]. Go ahead.

[THOMAS LECAT]: I did not want to speak for a second time, but since the issue of consent was brought up, I know that some registries are considering a consent-based response to GDPR. And I would just like to caution everyone who is considering that concept that this consent can be withdrawn at any time without giving reasons. And the question is, how do you carve the personal data out of your systems, particularly when it's distributed?

Also, there are legal experts who say that consent, once given, doesn't last for a lifetime. So they think that it needs to be

refreshed after a couple of years. So the preferable way potentially, the less contentious way for contract parties to deal with this might be to look at, where you have a legitimate purpose, to collect data and process data. And then you don't need that consent. But the exercise of assessing whether it's legitimate or not is quite complex, because you need to take every data element and assess it through the lifecycle, from collection to actually its deletion or its blocking.

Can go into more details on that, but just don't underestimate it. So if you have a reseller, then you need to look at the step between reseller and registrar, from registrar to registry, interface to ICANN, to the [EU bureau], to the escrow agent, and all that, and to look at whether the data can be passed on legitimately and whether it can be made available to, let's say, law enforcement or through public WHOIS for every data element. So it's quite complex. Start doing it now. I guess with the exercise that ICANN is doing, we're trying to work on offering assistance and guidance to the contracted parties to facilitate that process. But everyone needs to start looking at their own processes now.

CHERYL LANGDON-ORR: Thank you very much, [Thomas]. You took a couple of the things I wanted to say, in terms of complexity and next steps that I was going to do in summation, so that's done.

I'm now wanting all of you to do one more thing. And that's put your hands together to think what I might suggest is a nicely gender balanced, from my very biased view, group, and my two wonderful moderators. Thank you, gentlemen. The interpreters, we would not communicate without you. The IT staff, and those of you who I've ignored your names and given you station numbers all afternoon. Thank you, one and all. This session is now closed.

[END OF TRANSCRIPTION]