COPENHAGEN – GAC Meeting: Council of Europe Data Protection Commissioners
Monday, March 13, 2017 – 17:00 to 18:30 CET
ICANN58 | Copenhagen, Denmark

THOMAS SCHNEIDER: Hello, everybody. Please take your seats. And welcome to the special session of the GAC and the Council of Europe, which was initiated again by the Council of Europe, for which I would like to thank Johannes and his team, of course, which includes some number of real experts on data protection. And we also have a law enforcement colleague here, as we had in the session led by the GNSO just now in the big room.

I'll stop here. Because I think you don't want to hear me talk, but you want to have an interactive discussion with the experts on data protection and on law enforcement. Thank you. Johannes Kleijssen, please.

JOHANNES KLEIJSSEN: Thank you, Thomas. I'll be brief to give as much time as possible to the members of the panel. Just to thank the GAC for enabling this dialogue, this exchange of views with data protection experts.

We just had a very good cross-community discussion on this issue. And, from the reactions we see from the floor, it is clear that many think that this discussion should not be one-off but the beginning of a process.

In my introduction there, I presented the Council of Europe's -- the Council of Europe. But I think you probably know us, since we've now been an observer with the GAC since 2010 and have submitted three reports, the most recent one on human rights aspect of applications for gTLDs, which I know you have been talking about.

So I won't introduce the organization but just to stress that, for today's event, the debate that is going on is both timely and necessary. Increasingly, there is the risk and already a reality of conflicting obligations, contractual obligations, on the one hand, and data protection obligations, binding legal obligations on the other hand.

And, therefore, this discussion, as I said, is both timely and needed.

We come in as Council of Europe because, of course, as many of you will know, there is the data protection Convention 108, which has 50 parties and some 10 observers, which means that it brings together about half of the states in the world that have specific data protection legislation.

We also have -- my title, Director Of Information Society and fight against crime as an indication of that -- a very strong law enforcement community within the Council of Europe. We have a human rights convention in the court. But we also have some 60 criminal law conventions, some of them ratified by nearly 70 states worldwide, and our cybercrime convention, which has 50 parties as has our data protection convention. We cooperate on capacity building with some 125 countries. So we're very much beyond Europe's borders.

Thomas, if I may quote you for a moment to close, what you said at the cross-community dialogue. Data policy, you stated, is a key factor. If I may paraphrase you, it is a force for the good potentially. But, of course, there are huge risks. And, increasingly, data subjects -- that means all of us around the world -- are worried what happens to our data. You see many manifestations of that worry. And, for instance, the recent disclosure by WikiLeaks, which attracted global attention, was yet another example of the concerns.

Therefore, discussion within ICANN and the GAC with law enforcement is necessary, also with business and civil society. But I would like to add also with the data protection community. Thank you.

ALESSANDRA PIERUCCI: Hello to everybody. My name is Alessandra Pierucci. Let me, first of all, thank you very much for giving me the possibility to participate in this outstanding event. I'm very grateful and pleased to be here.

I'm here in my quality of the chair of the consultative commission, sorry, committee for Convention 108, which is the Council of Europe convention for the protection of personal data. The consultative committee is composed by many representatives from the parties to the convention but not only, also by observers, which actually take part actively in the discussion of our committee.

And our committee is, basically, responsible for the interpretation of the main provisions of the Convention 108 and of the implementation also of data protection principles in the various sectors at stake.

Just to give you an example, the consultative committee has adopted a number of guidelines, a number of recommendations, which, of course, have to be then adopted at the Committee of Ministers level, in data protection in various fields like employment, public sectors, profiling, health data, just to mention a few examples.

I would like now to draw your attention on Convention 108, in particular on two main features of Convention 108.

The first one is that we are speaking about the first -- and I will say also nowadays, the only -- binding instrument at international level for data protection.

I would say those that the second element which characterizes this convention is its open character, its openness, also to third countries. And I'm saying that because Convention 108 has not only been ratified by the 47 member states, as it was recalled before by Johannes Kleijssen, 47 members of the Council of Europe, but is also open to accessions of third parties.

That was the case, for example, as you can see in the next slide, of Uruguay of Senegal, which actually ratified the convention as a third party, and Mauritius. There are other countries also that are in the process of ratifying Convention 108, as you can see in the slide, Morocco, Tunisia, Cape Verde, and Burkina Faso.

The open nature of this convention is also due to the fact that we have, as I was saying before, an active participation of observers, both from international organizations and also from other countries like U.S., Canada, Australia, South Korea, Mexico, and Indonesia. And we actually just had the request by Japan and Philippines for a total of over 60 countries contributing to the work of our committee.

Next slide, please.

Well, even without the slide we continue just giving you some hints regarding Convention 108.

Convention 108, as it happened at the European Union level, underwent a process of modernization.

That was due to the fact, as you can imagine, that the data protection principles contained in Convention 108 had to be a little bit updated in respect of the impact of new technologies and globalization.

This kind of modernization process started with involvement of many stakeholders. It was actually -- the opening of such process was a consultation. And we received a lot of contribution from many stakeholders, including the private sectors.

At the moment it is up to the Committee of Ministry of the Council of Europe to finalize the process of modernization of this instrument.

I will spend just a few words saying what, basically, remains valid of the general structure of Convention 108 and which are the new elements of convention -- of the modernized Convention 108.

I would say that the general structure, the fact that the convention speaks with a universal language is still valid for the

modernized convention as it used to be in the, let's say, old convention. It speaks with general principles and not detailed principles because it has to speak with a number, very big number of countries. It has still a technologically neutral language in order, of course, to avoid that it becomes obsolete too early. And it ensures consistency with the European Union framework.

I think it's important to give a few words on that. Of course, there's a bridge between the Convention 108 and the European Union, data protection framework which has been actually emphasized by the new EU regulation, which, in a specific recital, specifies that the accession of a third country to Convention 108 is actually an element which can be considered as being important for the evaluation of adequacy of a third country.

Other elements which have been, let's say, strengthened in the process of modernization of Convention 108, as you can see in the slide, is first of all proportionality and data minimization. This is actually a crucial principle for data protection. Accountability was also in the new text of the convention, which means that data controllers and data processors must ensure the compliance with the data protection principles on paper but also in practice. Transparency has been enhanced, which means that data subject must be aware of the processing of

personal data related to them. And they must be aware of that also in order to exercise their rights, which has been -- which have been also strengthened in the new structure of the convention. Convention 108, for example, now has introduced the right not to be subject to automated decision without having the possibility to give his or her personal view.

Security of data is another element which has been strengthened in the new convention. And specific provisions on international data transfers and supervisory authorities have been also included, whereas these two topics are, at the moment, part of the additional protocol of Convention 108.

Next slide, please.

Okay. So that was just a very general overview of the main principle of the Convention 108. The message I really would like to bring you is the willingness of the consultative committee of Convention 108 to open a dialogue with ICANN, and let's say act as a possible interlocutors in case privacy concerns and questions may arise.

I have already emphasized the fact that the consultative committee is quite used to work in a kind of multistakeholder environment and very much open to countries all over the world. So once again, we would be keen to contribute to such work.

Thank you very much.

THOMAS SCHNEIDER: Thank you, Alessandra.

Next we have Joseph Cannataci from the United Nations. He's the presidential rapporteur on the right to privacy. Welcome to the GAC.

JOSEPH CANNATACI: Thank you very much, Thomas. I think those of you who were in the previous session would understand why it's so easy for me now to follow on from Alessandra's presentation, because we have two organizations, the mommy organization, the Council of Europe, and the European Union, which came later but which actually took over. And we've got to keep a bit of history in mind, ladies and gentlemen. It was the council of -- the convention that Alessandra has been talking about has been going on since 1981 and is about to receive a further modernization. And it was that convention which inspired the European Union. It wasn't yet the union then, when in June of 1981 it wrote to its then, wait for it, 7 to 12 members and said, "Hello, the Council of Europe has just done this. We think it's a good idea. Why don't you sign up?"

And not enough members signed up, and so what happened then was that they quickly -- they -- well, not quickly. Between 1990 and 1995 came out with a directive, EU directive 46-95 which has now been modernized into the GDPR, the General Data Protection Regulation.

And I think that context is very important because whereas, looking at things from a global perspective, look at it from those countries outside Europe, they receive one kind of impetus from the GDPR. So companies in those countries who want to do business in Europe have the GDPR pushing down to see how they're going to comply in one way or another, whereas the governments in those countries who would like to move towards a regime that is more structured in a privacy friendly point of view would tend to go towards the framework which is provided by the Council of Europe which Alessandra has just outlined.

And I think that that first part should also remind us of other initiatives which have been taken which then look to transport of data flows and the police.

I'm sure if we go outside the discussion which is of more direct interest to corporations and then go to that part of the discussion which deals with the public, or the public sphere, the transfer of data for two reasons: the police, law enforcement; and also intelligence services. And let's talk about it. And

perhaps -- I don't know if Caroline will be coming in on this later when she talks about the framework that already exists within INTERPOL. But first of all we should talk of another convention, the cybercrime convention.

So there are another 44 to 50 countries, I haven't checked exactly is standing today, but at least 47, possibly going towards 50 countries which are signed up to the Cybercrime Convention, Convention 185. And there are -- there is part of the convention, Section 32, which is intended to facilitate the transfer of data between one authority and another. That part is being modernized. There have been discussions going on for several years on how best to achieve that.

If you feel there's a "but" coming, that's because it's true, there is a but coming, and the but is that that convention, with all its good things and all its imperfections is only designed to achieve one thing, and that is data protection -- that's data transfers in the law enforcement.

If you look at Section 14 of that convention, it is not designed to handle intelligence. It is not designed to handle exchange of data outside the police sector.

And I think it's important for us to remember because many of you people will be faced by customers or whoever come along and say, "Ah, but Edward Snowden said this, and our data is is

happening that way, and this is what's happening in the terms of privacy." And in reality, the Cybercrime Convention is not designed to tackle that point, which is why you will have seen that -- in the report that I presented to the United Nations Human Rights Council last week, I have spoken of efforts which are ongoing to outside the U.N. at this moment in time, but which may possibly be brought inside the U.N. sometime next year which deal with preparing another agreement, another part of possibly a salami-slice approach to cyber law which would be a legal instrument governing surveillance in cyberspace. Essentially what I'm talking about is I'm saying, okay, we have an attempt to tackle, we have an attempt to tackle cybercrime in the Cybercrime Convention. We have an attempt to tackle the personal data held by corporations and governments in the context of countries which have joined Convention 108. But what about the rest of it? What about the rest of cyber law?

And this is something we have to look at. It's not going to be something easy to solve, but, hey, there are many other examples of difficult things which the world has solved. And that's surveillance in cyberspace.

It's of particular interest to people at ICANN because of course people at ICANN are involved in all kinds of requests; right? Who is requesting the data, especially when it goes government to government, intelligence service to intelligence service. But

more importantly sometimes, hello, I am corporation X. I have a data center out in Germany, and then there's some funny one in court in New York who wants -- who wants me to -- who is asking to give you the data I have stored in Ireland or in Honolulu or in India. What am I going to do?

And if you're at the receiving end, whether as a government or as an ISP or as a data center controller, how do you handle this. And what's more, what are the kinds of technical safeguards that should be put in to either facilitate this kind of exchange or to make sure that it doesn't happen in a way which is abusive?

And I'll conclude by reminding you of a couple of things. Not only must we be looking at identity management from a different perspective, but we could also be looking at other trades. We could also be looking at a whole bunch of things, a whole bunch of safeguards which could be called upon to implement to make sure that we are creating a more privacy friendly atmosphere in cyberspace, one which would encourage the growth of trust, especially, and increase in trust from the citizens' point of view. As I said last week, this would be good for privacy, it would be good for ISPs, it would be good for citizens, it would be good for governments, it would be good for business.

Thank you.

THOMAS SCHNEIDER: Thank you very much, Joseph Cannataci.

Next is Ms. Caroline Goemans-Dorny, data protection officer of INTERPOL.

CAROLINE GOEMANS-DORY: Thank you very much. Thank you very much for having invited me here.

Actually, last week there was at INTERPOL the Annual Conference of Head of National Central Bureaus meeting, and one of the -- it's the annual conference where, in fact, that serves as a brainstorming where brainstorms are much easier than perhaps during the General Assembly when there are more hot-potato issues to deal with and elections and that sort of things.

So there last week was really a brainstorming, within, in fact, the 190 member countries that had been invited. As you know, INTERPOL is a global organization. The global -- global organization for police cooperation, and covering 190 member countries. And one of the tasks is really to be -- to serve as an information hub for global police databases.

And one of the panels was on -- was on how strong data processing -- strong data processing standards, which was a

multidisciplinary panel. They asked me to intervene and asked me what I thought was the added value as INTERPOL data protection officer, the added value of strong data protection standards.

And now I'm not going to tell breaking news, but rather go back to the basics that for effective policing, you need -- you need basic trust. And this is where data protection framework can really help, not only to create that sort of ecosystem of trust within which police cooperation can effectively cooperate, but it's also a matter of reputation because it's -- as you may know, the INTERPOL's constitution refers expressly to the Universal Declaration of Human Rights. This concerns not only the right to privacy but also other rights, such as the right of freedom of expression. And there, INTERPOL really acts as a clearinghouse to review legally and also the quality of the information of the requests for cooperation that are sent in.

But -- So at INTERPOL, since long, since 1982, data protection regulations have been put in motion. The long-term investment and the belief in long-term added value of data protection is something that has been granted since a long time. It's like building -- taking time to build strong foundations for a solid building.

The first rule -- the rules of INTERPOL are, indeed, based on the principles of the Convention 108, which has universal outreach. And over the years, the rules on data protection were elaborated, were updated, were adapted, were refined, all the case law of the Office of Legal Affairs was put in it so that we ended up in 2011 to a real code where -- that we thought was a very good guidance for a police officer, and that was pretty detailed where they could really find an answer on all their questions.

So data protection is really a dynamic process. That's another point that INTERPOL has always taken for granted; that these rules have to be continuously updated. The first one, as I said, were in 1982. Even since our latest update of 2011, we had already two other ones. So I counted a couple of days ago, and it makes us an average of an update of every three years.

Then to keep up with all our challenges, we are already thinking about a new version on specific topics, like cooperation of the law enforcement with the private sector. There has been a huge evolution on that, whereas in 2004 law enforcement did not want to under- -- to hear about any cooperation with the private sector. This has changed a lot, and there we really need to have a framework.

Now, the way how we tackle new -- new issues is not to immediately have new rules. We prefer to set the projects that are very -- that are -- that are well framed, see -- evaluate those projects after a year, and then perhaps these experience can serve as a food for thought for eventually re-elaborate our rules and rethink our rules. This is how we have been working so far, and I expect that in a couple of years, very soon, our rules on working with private sector will be changed as well.

As I said, INTERPOL really acts as a clearinghouse. That's an important aspect. That the quality is reviewed, and that legal -- legitimacy is reviewed, and especially for what INTERPOL calls their notices. These are international alert with the purpose to -- with the purpose to arrest or to locate wanted persons. So very privacy intrusive; reason why there should be a closed review before they are published or -- or on the restrict website or eventually on the public website. There are specific criteria and thresholds for that.

I think the -- Beside these dynamic rules, there is also the advantages, of course, that the rules are global. They have a global outreach. Everybody finds himself in those rules, and so they create really a sort of interoperability between 190 member countries. They are based on several pillars. It's all well to have rules, but they have to be effectively implemented. There is

effective oversight. We foresee regular trainings and redress for individuals.

Important in all that process to build a kind of system, not only based on rules but really also business processes and technology, is the rule of 190 data protection officers that are appointed in each national central bureau of each member country of INTERPOL. It's -- I have the privilege to coordinate their work. It's, of course, ongoing work. It's very exciting work. They are really very happy to be appointed as data protection officer. And I think this can really leverage the global threshold of data protection worldwide.

So as I said, I think, frankly, we have to think -- to think the implementation of privacy principles and data protection principles as really a multidisciplinary area. Not stick only to legal. Not be overexcited about legal only. The business processes are so important. The choice of the right technologies. And after all, as I said at the last -- the previous meeting, we're speaking really about principles of good governance. Accuracy is about what are you processing. Why are you processing? That's a purpose principle. How are you processing? Compliance. These are all good governance principles. And when you have good governance, you have good business.

So I would say data protection at INTERPOL is really an ongoing work since years and years, and that is -- but it is -- it is really seen as a basis for trust and for reputation of the organization.

Thank you very much.

THOMAS SCHNEIDER: Thank you, Caroline Goemans-Dorny.

Next is Giovanni Buttarelli from the European Data Protection Supervisor.

GIOVANNI BUTTARELLI: Thank you for your invitation to join this panel. I don't want to repeat myself for those who attended the previous panel.

One question you may have listening to all of us is are we Europeans dictating our rules to the rest of the world?

It's a legitimate question. But I think if we analyze all the details and all the relevant elements, you may easily conclude that all these examples, I think, and different pieces of legislation. And, therefore, from Council of Europe, European Union, APAC countries, show the growing interoperability of a modern notion of data protection, which is now interesting and affecting 120 countries in the world. Professor Greenleaf has analyzed the philosophy of these horizontal pieces of national legislation.

And the outcome is that, even outside the European Union and outside the Council of Europe framework, more than half of these 120 countries -- and we're speaking about South America, for instance, Africa -- are following a model, which is not distant from the European one.

So it seems that there is a growing concern about the need to have a common answer to the same problems.

And I see a trend where we would like to depart from legal requirements in terms of useless formalities to effective safeguards.

So this is the objective of making data protection digital and by preserving principles and values and by making them more effective in practice in society where we administer our entire life via a smartphone.

And the real challenge, for instance, the European Union, GDPR, is to make it effective in the big data world. No one will change in the GDPR before 20 years. And, even if someone will start by making proposal, it will take years for discussions and enforcement. So the piece of legislation we are dealing with now, which will be fully applicable from the 25th of May next year, will last for at least 20 years, which is more than a century.

And we have to then consider the long-term expectations. My view is that we will see soon the notion of personal data disappearing. Everyone will become in the big data world easily re-identifiable. So the notion of anonymity will remain something for the books.

Another important trend to be considered is the flexibility of the European Union approach. We speak about rules, legal grounds, principles, *** okay.

What about the 25 provisions in the GDPR allowing independent regulators to speak one voice and to issue guidelines to certify processing categories or processing of personal data and, therefore, to have an additional set of inclusive regulation based on consultation. This offers a lot of space for interesting specificity and also to be inclusive since independent regulation will have a chance to interact more with relevant stakeholders.

What we are offering in return of this, I mean, serious legal framework, based on serious administrative facts, first of all, more harmonization. We would like to speak more with one voice within the 28+1 independent data protection authorities. So this regimented approach building on the 1995 European Union directive will easily and rapidly disappear.

We're offering a system which is now to be completed by the ePrivacy regulation, which is an essential piece of legislation for

data controllers working in the area of public available communication networks, we are offering a system based on technologically neutral provisions.

We would like to -- I mean, allow every data controller established outside the EU operating from third countries, one from number to code. And this is why we're deeply committed together with other callers to build the so-called consistency mechanism to set up a suitable system for mutual assistance and joint operations so that operators interested to work in more than one country in the EU should not, I mean, approach different authorities.

We're deeply committed to reinforce international cooperation. And our Web sites document how we are in touch with sister authorities in the world but also with international organizations not subject as such to data protection principles.

Finally, let me say that the European contribution to the international debate on data protection would like to also be complete and coherent. So there is an answer to growing concerns about the consistency of this legal framework with other relevant pieces of legislation such as those on copyright, on consumer law, and the digital clearinghouse initiative launched by my institution, the European data protection supervisor, is a clear example.

And we would like not to leave you alone before law enforcement bodies. This is why the GDPR is accompanied by another important piece of legislation you should deal with --

because this is directly relevant for you -- a directive for cooperation for police authorities and judicial authorities which has to be implemented at a national level in all 28 member states by the 6th of May next year. So it means the way, which, at least from one of the European countries, you will be approached in case of a collection of data for law enforcement purposes will be more based on principles of proportionality.

Please, also consider, in addition to what Caroline said about INTERPOL, that Europol, the so-called European Union FBI, will be subject to a new regulation which will enter into full application by the 1st of May this year. And my institution, in cooperation with other national DPIs, will be in touch for the relevant enforcement.

So I think we have a lot of input to consider in this global dimension. My recommendation is to, yes, consider the dimension of transfer of data from the EU where we have heard about this project of transferring data to VeriSign in the U.S. But please consider also -- by legal viewpoint, let me focus on the provision -- the scope of application of the new GDPR, which not only applies to transfer. Transfer is a processing operation. But

the GDPR will be applicable in its entirety to all set of processing operation, including the collection, the elaboration, retention of data. So a company established in Japan and in the U.S. will be subject to the GDPR regardless of the moment where data transferred outside the EU, provide that they will offer good and services in the EU.

So the key point will be location of -- I mean, the location where the data -- the services are offered.

About transfer, there are still unclear perspectives about the, let's say, the layer of safeguards. Recently the Court of Justice has said that the principle of adequate protection of personal data means, after the Lisbon treaty, that the safeguards to be offered in a third country should be essentially equivalent. This is something that we are all analyzing.

Other decisions are coming, for instance, those concerning the Canadian PNR. And they will be horizontally relevant. As well as the famous decision on digital rights versus island concerning telecom, operators and Internet operators which contains useful tips for all of you.

So a little bit of work in progress, but also a lot of clarity and a lot of flexibility. So we are all committed to deal with our regional legislation but in a global perspective, because the answer should be necessarily placed at international level.

THOMAS SCHNEIDER: Thank you, Giovanni Buttarelli. Next we have Mr. Wilbert Tomesen who is the vice chair of Article 29 working party. Thank you.

WILBERT TOMESEN: Thank you very much. Since Giovanni and I are colleagues in the community of data protection authorities in Europe, I can easily echo his comments, of course. So I think I can be quite short.

I'm thinking back of there's a picture of Obama on the first -- President Obama -- on the first floor. And, if I remember well, he's quoted by saying something like, "I'm not bringing you fear. I'm bringing you the future."

What I would like to -- it's true. We in Europe are not living on an island, obviously not. And the things we're doing as it comes to privacy and data protection fits in with what's going on in the world more or less. But we have brought it into real law. And we are granted with enforcing powers, DPAs, and with penalizing powers.

But it goes back to the core of what we're talking about, and that's what I'm very much convinced about. It's about the way we in the data-driven world that we are living in now and heading for even more, the way that we handle each other's

data. And I'm in this business since five years now, something like that.

And I'm very much convinced about the need to do it fair, to do transparent, and to be as predictable as you can only be. The reason I called it in before, as Tim Berners-Lee said this weekend at the occasion of the 28th birthday of his more or less invention of the Internet, he said, "Haven't we lost control over our personal data?" And more or less what we are seeking for in Europe is an answer to that question. If we have lost control over our personal data, how can we get it back? That is my approach. So, yes, we are talking about enforcing powers and penalizing powers.

What my message to you is ask yourself why am I collecting data? What am I collecting it for? What's the purpose of it? And, while I'm doing it, am I clear and am I transparent to the data users? Do I have to do it is another way that is less infringing?

And, as Giovanni, basically, has been saying, I see it as my duty. We see it as our duty to assist you, when necessary, to answer the difficult questions that, obviously, come with it.

But the principles are not that difficult. The principle is why am I doing this? Am I allowed to do it? And am I, basically, just being fair? Thank you very much.

THOMAS SCHNEIDER: Thank you very much. So we have some time for a, hopefully, interactive exchange.

So I would like to give the floor for questions or comments to the members of the GAC and then, hopefully, have a good discussion. Yes, the Netherlands, please. Please present yourself, as people may not know who you are.

NETHERLANDS: Thank you, Chair. This is Thomas de Haan, from Dutch Ministry of Economic Affairs and the GAC rep for the Netherlands.

I have a question for Mr. Buttarelli because I was very glad, not only in this session which expressed this assistance or, let's say, all you can contribute from European side for the interpretation of the new GDP`R for next year.

And I want to go back to the earlier session, which is, I think, very positive. I think many in the community expressed or at least applaud also to the request that you -- and let's say with your expertise in your organizations also really assist ICANN in the privacy domain. I think the privacy domain is something which we, as GAC, are -- it's one of our main public interest issues for our citizens. I think we should very much be aware of all the potential breaches, potential squeezes within, let's say,

the ICANN remit of the ICANN contracts with registries, registrars, et cetera.

And I want to go back to the issue which was slightly very shortly presented in the former session which is, basically, the squeeze in the registry agreement which has been signed for very many gTLDs.

And I remember gTLDs were originally conceived as a concept by .BERLIN in Europe. And there are many, many Europe gTLDs now functioning.

Also we have Netherlands .AMSTERDAM,

.FREISLAND, .FRL. And, basically, we're already aware of the real squeeze of two clauses. I'm just talking not about data transfer but just only talking about the publication of data and the ways which already gives a problem, two clauses which say you should abide and comply to international law and you should present this data.

This, alone, is already a problem.

So what I would like to ask you is there a possibility in which, before the GDPR gets into implementation in May/June '18, could, from the European side, there be given some clarity then about whether the implementation is according to the GDRP,

meaning that then ICANN could have ample time to also change the contracts accordingly?

And I would -- but this is not addressed to you, but to ICANN. I would also urge ICANN to really suspend the compliance upon the basis of the old contracts.

So this is my question. Thank you.

GIOVANNI BUTTARELLI: Also on behalf of Wilbert -- and I'm speaking under his strict control -- the answer is yes. The full implementation of the GDPR cannot be improvised. But 14 months can be used in the proper way.

We are a lover of the ICANN system. And we would like to help you to match the objectives with -- I mean the novelties by legislative viewpoint.

We have no alternative. The problem does not relate to the GDPR. Because the GDPR is simply a transposition of a legal obligation contained in Article 16 on the treaty of the functioning of the EU, according to which data protection is now something new, is a fundamental right separate from privacy. So the way in which the data is processed by someone else, even if data collection is mandatory, even if they are to be published and made publicly available, everyone in the world is part of a

fundamental right so is subject to scrutiny and to -- I mean, a legal ground. The legal ground is mentioned in the treaty. It is the constitution in the EU. The fact that consent is to be freely given as well we have the charter.

So this is a novelty which is to be considered.

Let me refer to another example which appeared to be a couple of years ago unsolvable.

The WADA system used for anti-doping services. They started by saying we have to comply with many nodes in the world. We cannot simply deal with the European one. So I make the story short at the end. We have identified the solution with full success because we would like to -- we are not expert on what you are doing here, but we can be of a help in translating these principles into practice.

But what is key is that there is an honesty and flexibility in identifying first the purposes, availability to identify the less intrusive means to achieve the purposes, and to refrain from wide publication where not necessary to distinguish what is useful and what is necessary. What is necessary for registers, registries, and what is useful for third parties -- for instance, intellectual property rights or law enforcement bodies.

If we have such honesty and flexibility and identifying what the real problems are, I think data protection authorities may be of a help legislating this into -- into practice. Or the alternative is to have a leading case in 18, 20 -- for 24 months from now when someone will submit a complaint or one DPA will start an enforcement action ex officio. This is something we would really like to prevent, and this is why we are here today.

So on behalf of the other colleagues, we look the liberty today at lunchtime with members of the ICANN Board to suggest that perhaps as some of you may approach the community data protection authorities come with -- I mean, carry the doleance or request for assistance and allow us to simply be of a help. Today we cannot solve all the problems here in a panel. We can simply confirm our availability.

WILBERT TOMESEN: Maybe I could add one thing. Last week I was at a conference also, and it was about transparency. It's basically the way that we inform data subjects. Are we concise? Are we comprehensible? Do people know basically what we are asking of them and why?

And the discussion came at a point, and I'm not here now to only give the answers that are favorable to you. The discussion entered into a situation that I had to say, listen, if you are not

able to explain to your customers, to your citizens or whatever why you are processing their data, for what reason, to be concise and clear about that, then maybe you should either hire new communication experts or just stop processing that data. And this would also be an answer, beside what Giovanni very rightly has been saying. If processing of data can't be brought within the framework of our future law, which basically is codification of principles that we have been knowing for decades now, if it can't be brought within that framework, you should basically, I'm afraid, more or less rethink the processing activities you're undertaking.

So at the end of the day, that's the law. Those are the principles. You have to be clear about it. You have to be able to explain it. And it has to be within the context of the GDPR.

Thank you.

THOMAS SCHNEIDER: Thank you.

Further questions or comments?

Yes, Belgium.

BELGIUM: Thank you, Chair. I'm the representative of Belgium for the GAC. I'm also a member of the Belgium privacy committee. And this is not a new topic, of course. We have been discussing data protection issues within GAC for many years. That is why I celebrate your presence today.

I'm glad to see that today we have this opportunity to reach out to you to ask for your help to clarify certain aspects.

I would like to know whether you have already had some interaction with ICANN, because sometimes we give advice to ICANN, and when we give advice to ICANN they listen to us and sometimes they don't. But which would be the general common principles that we should push from the GAC in terms of data protection and privacy for ICANN to take them into account? For us, it would be very useful if you could identify for us which are the main provisions that would be contrary to the general principles that are included in the contracts with registries and ICANN.

I would like to also ask you whether you have had productive exchanges with ICANN.

THOMAS SCHNEIDER: Yes, Giovanni.

GIOVANNI BUTTARELLI: Not yet, and we are waiting for some positive answers.

My -- my predecessor a couple of years ago sent a letter, for instance, on data retention. And, I mean, no one of the suggestions we recommended have been taken on board.

We adopted an opinion 14 years ago within the 29 working party. It has been commented, but we are still waiting for, I mean, a positive outcome.

In 2013, together with other European Union authorities, we adopted the opinion number 3, 2013, on purpose limitation, which is extremely relevant for you and may be helpful. And again, we are only here today to start with the relevant discussions. So I can simply say we continue to be available. As a piece of information, let me say that EDPS together with a rotating co-host every -- I mean, two years, organize an international event or international entities organization, not subject, as such, to data protection provisions.

Here we are in between, I mean, duties of ICANN in general terms as an entity and also duties and obligations of single data controllers following the ICANN policy.

But in case ICANN would be interested to join us, please consider that early May we will have the next event in Geneva. I think it's the 11th and 12th. All the details appear on the website of my

organization. We will be very pleased to host you. And you will see how other international organizations not subject to such national laws are sharing experiences in terms of implementation. So that's a moment also for creativity, to understand what others are doing. We're not adopting decisions. It's simply a moment for sharing and for -- I mean, for building on what others are doing.

THOMAS SCHNEIDER: Thank you. Before giving the floor to Tarek, just to add that the board has signaled high interest in engaging with the data protection commissioners and has had a lunch, as you've heard, today earlier. And this is -- Everybody agrees that this is the beginning of a more intense, a more regular exchange, as it has been in the past years. As we've heard in this session before, there have been some context, but those haven't been. So I'll let it close. But let me give the floor to Tarek from ICANN. You may refer to the fact that the board has a meeting --

TAREK KAMEL: Exactly. I was going to say the same thing that Thomas has said, that we had a very constructive meeting with the board, and the board chair, Steve Crocker, has signaled clearly on behalf of the board clear welcome to the presence of the commissioners and that this is the beginning of a constructive dialogue and working

together with the community and with the board and definitely the different constituencies, the GAC and the GNSO, to see how to take this forward.

And I think that we will see concrete steps from ICANN's side and ICANN's board very soon to respond to the positive reflections that came today from the European Commission and from the Council of Europe.

So thank you, Thomas, for giving me this opportunity to confirm that we'll not wait another 14 years until something happen.

THOMAS SCHNEIDER: Thank you, Tarek. Giovanni, please.

GIOVANNI BUTTARELLI: Just to say also on behalf of Wilbert, because of conflicting commitments, Wilbert and I perhaps are the only one in the panel forced to take a cab to the airport in no later than ten minutes. So if there is place for, you know, one or two more questions, we will be pleased to answer, but then apologies in advance because our departure.

THOMAS SCHNEIDER: Yes. Russia.

RUSSIAN FEDERATION: A question to Alessandra. Or maybe not a question. A proposition. You mentioned at the beginning of your speech report of Council of Europe about human rights in a new gTLD. We discussed it maybe Saturday. It was useful and really valuable report. And it provide for us some insight and external expertise.

Can we maybe plan to do the same work for the personal data protection in ICANN procedures? Or if you haven't plan, it can be maybe its proposition to do such analysis and such audit to be a good support for us, because I'm a little bit involved in question related to privacy, personal data, protection and digital identification. It's quite complex thing. And any valuable, external, external analysis from expert is useful because it's a little bit as a point of view. It's always valuable.

THOMAS SCHNEIDER: Johannes.

JOHANNES KLEIJSSEN: Thank you. It was actually me who mentioned the report on human rights aspects of applications for gTLDs. And thank you very much for the suggestion. Today's meetings, exchange of views, where based on our proposal, Council of Europe proposal, supported by the different ICANN communities. We

would be very interested in submitting to the GAC a report on -- on the -- on various aspects of data protection within -- within ICANN. And the reactions we've received so far, in addition to yours, are encouraging in this respect. So we'll certainly look into this.

Thank you.

ALESSANDRA PIERUCCI: Maybe just to complement. I can reassure you that the discussion here will be definitely reported to the consultative committee as it is actually has been already done during the years. Because, I mean, we have been following the work of ICANN, and there was a constant communication with the members of the consultative committee. And thank you very much for your proposal.

Thank you.

THOMAS SCHNEIDER: And just -- just to add to what Johannes said, for those with a little shorter memory, the Council of Europe has commissioned a report on human rights and new gTLDs. Not on community TLDs but on human rights and new gTLDs in 2014 that was dealing with freedom of expression and freedom of assembly and with data protection. And I was one of the co-authors of the

two co-authors of that report. So that is -- if you go through the archives, that is from 2014. And if you don't have it or don't find it anymore, you haven't been in the GAC at that time, of course we can organize a copy for you.

Thank you.

Other comments? Questions?

Yes, Cathrin.

CATHRIN BAUER-BULST: Yes, thank you, Thomas. Cathrin Bauer-Bulst, European Commission. I also have the honor of being one of the co-chairs of the Public Safety Working Group of the GAC. And I just want to pick up something that was said in the earlier session about how law enforcement and data protection never meet. In fact, they do all the time here in the GAC, and that's a lot of the work we do here quite successfully and where we also have a lot of aligned interest, in fact, across law enforcement and the data protection community, such as working on the accuracy of the data that is available and working on preventing misuse of data.

And I would just like to encourage you, as in the public safety group we have also worked, we've spent a lot of time on these concepts and on trying to basically work on creating a system that can, at the same time, accommodate the legitimate

interests of law enforcement, both civil and criminal, which often also focus on the protection of human rights, such as the right to life and the right to human dignity with the legitimate interests of data protection.

So we've had several presentations on data protection principles and how these can be utilized, for example, in the new process for the policy development around a new RDS system. And I would just like to encourage you, from the perspective of both the European Commission and the Public Safety Working Group, is to actively participate in these processes also by being present here and having these conversations also in the policy development processes, because what we find is that it's extremely difficult to translate these abstract principles, such as purpose limitation, the proper definition of purpose, into something that can be workable in a policy here at ICANN.

And what I personally see is that there are a lot of opportunities for synergies where these principles could be picked up and could be translated into workable framework. That is not yet happening because there is sort of a disconnect between the positions that have been taken sort of from the outside and the work that is happening here.

So I can only encourage you to be more closely involved and to continue your participation also in the Public Safety Working Group and in the policy development processes here.

Thank you.

THOMAS SCHNEIDER: Thank you.

Further comments? Questions?

Yes, EBU.

EUROPEAN BROADCASTING UNION: Thank you for the floor. I have a question for Professor Cannataci because we have heard quite a pessimistic vision of the future from Buttarelli saying that with the big data it will be practically impossible or near impossible to keep the -- our secrets, let's say, in what we do, et cetera. So do you share this view or is something that is still manageable in order not to happen?

JOSEPH CANNATACI: This is not going to be a lawyer's answer, but it is yes and no. We -- if we continue -- Let me preface something. Firstly, I should point out or remind the colleagues in the room that wearing my U.N. special rapporteur hat, I have set up a task force, one of five

on different subjects, but big data and open data is one of my list of priorities. And one of them, big data and open data, is one of the first which I hope we'll be able to report sometime between January -- I'm sorry, July and October of this year.

The -- That being said, in other words that caveat is this is something that we're looking at very carefully, everybody is talking and doing something about big data. The Council of Europe has just come up with guidelines on it. Last Friday, the information customer of the United Kingdom has just published a new report on it. So we are working on it at the U.N. level.

I think that the pessimism, if any -- I think, frankly, that Giovanni was just being realistic rather than pessimistic -- depends on what we're going to do about something else. I think it's wrong to just talk about big data. I think when we talk about big data we should be talking about two other things, but certainly one other thing, and the first is open data; right?

You see, big data cannot be such a menace to privacy unless it also can -- until -- unless big data analytical approaches can also take advantage of other data sets. And especially what we have to look at is those data sets which are put into the public domain by public authorities which originally collected that data.

In many jurisdictions across the world be what I see are databases, the social security and health especially, which were

originally put together for one purpose and now somebody's come up with the bright idea, aha, we can provide a huge benefit to humanity by putting them in the public domain. Now, you tell me how you're going to come to that argument. The minute you say I'm going to put a great benefit to humanity. Obviously they're forgetting the small print, which is as soon as a private company starts taking advantage of that data, which has been put into the public domain, the first line of processing and it becomes intellectual property which belongs to somebody else. That seems to be forgotten by a huge bunch of people who have been either actively lobbying for that or else on the government side who fail to see it, or perhaps they did see it.

So, actually, I think that if you cut down -- if you stick by the original principle that data collected for one purpose should not be released for another purpose, and if you do not release huge amounts of data into the open data ecosystem, then actually you have good cause to be less pessimistic.

Also why because growingly, if you look at the way that the GDPR and other areas of laws are concerned, will be applied around the world. That part of data protection will, hopefully, be more effective.

Why do I say, "hopefully"? Because, actually, big data is in GDPR, in my mind, one of the grayer areas. What can actually be

done? Is anything which is called statistical for research, can we get away with it? There's actually a delegation of international authorities rather than having a top line regulatory approach.

So I think that, if we have a rethink about big data and open data, and, if we refine our approach there, I would be less pessimistic.

That being said, there is a lot of pressure from a lot of quarters on a lot of politicians to say "yes" to big data and open data.

Right?

And I have seen countries over the past 18 months where, even with tiny villages and tiny towns, relatively small countries, you know, smaller than Denmark, where big data is being touted as a huge useful tool for social services.

Frankly, if you're a social worker in a small town and you don't know who your problem clients are, you don't need big data. You need a bigger approach to your pension day. Because this just -- the amount of arguments and silly arguments that have been advanced for big data and open data are incredible. They have to be seen to be believed. And for some politicians to have swallowed them really makes me scratch my head. That being said, there is no doubt that big data analytics can be useful to humanity, especially in some areas like health, et cetera. But it's

going to be done, you know, very carefully indeed. And I hope that we can bring together some strands of research over the next few years in order to be able to answer your questions in a more positive way.

Thank you.

THOMAS SCHNEIDER: Thank you for this very interesting answer. Alessandra wanted to answer something.

ALESSANDRA PIERUCCI: Just to give some additional information and to echo what Joe was saying. Of course, big data has actually introduced challenges very difficult to solve. The Council of Europe, as Joe was mentioning, actually adopted -- the consultative committee adopted guidelines in early January on big data where, basically, it acknowledged the fact that even the traditional principle of data protection are challenged. Information, consent, even the principle of purpose. And somehow the guidelines urge legislators to try to get out of the traditional notion of individual control over his or her personal data and opt for a different approach, let's say a multiple impact assessment of the risks of big data, which, of course, gives a lot of

responsibility on those operating on big data. Also in terms of the evaluation of the ethics of big data. Thank you.

THOMAS SCHNEIDER: Yes, Caroline.

CAROLINE GOEMANS-DORNY: Just also about big data in the future, I think that, as we said earlier in other panels, technology will be very important. Technology is neutral, but you can use it both ways. It's not, per se, privacy intrusive. It can also be privacy enhancing.

If we think, for instance, to this -- the first -- the first scanners of the body images at the airports for the safety of the passengers, the first one were just terrible. It was a lot, very controversial. Now privacy filters have been installed. The body details are blurred. And the elements, dangerous elements are highlighted.

So you reach the same -- the functionality is the same. The safety and the purpose of the safety of the passengers is reaching both, but the technology has adapted.

So it will be hugely important to have this mindset of privacy enhancing technology, that you can use technology to enhance privacy.

THOMAS SCHNEIDER: Thank you.

Further questions, comments?

If that's not the case, I think we've had -- all had a very long and interesting day.

And, as I said already in the meeting before, as I happen to be responsible also for the organization of the Swiss part of the organization of the IGF in Geneva, I think this is one of the issues that will for sure be at the core of the discussions in Geneva. Whether or not this is focused on ICANN issues is something to be discussed. But it may -- given the number of workshop slots, it may actually be one option, if some representatives of the ICANN business world, together with other stakeholders makes a proposal for an issue to be discussed, that may also help to speed up finding solutions for the ICANN-related aspects of this challenge. And, of course, the other, let's say broader challenges linked to big data and privacy in general. They will definitely be discussed on very many occasions in Geneva.

So, with this, I think I'd like to thank, again, the Council of Europe and, of course, also the U.N. special rapporteur for coming here and the INTERPOL and hope you have a good evening.

For those who can stay, I think there's the gala event going on not too far from here in the same huge building. Actually, those who have not yet gotten the invitation, I hope we can do it still because I didn't have the time yet to go and get it myself.

So thank you very much. And see you later in the other side of the building. Thank you.

[Applause.]

Thanks to ICANN for facilitating this, of course.

[END OF TRANSCRIPTION]