ICANN Transcription – Abu Dhabi
GNSO – Internet Service Providers and Connectivity Providers Constituency (ISPCP) Open Meeting Part 1
Tuesday, 31 October 2017 15:15 GST

Note: The following is the output of transcribing from an audio recording. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

On page: https://gnso.icann.org/en/group-activities/calendar

Wolf-Ulrich Knoben: So good afternoon. Welcome. You he talked to some - welcome to the ISPCP Constituency meeting here in Abu Dhabi. Welcome to the members and to the guests here.

My name is Wolf-Ulrich Knoben. I'm the Chair of the ISPCP Constituency and before we go through the agenda I would like just to go quickly around the table, and just everybody is going to introduce him or herself. Please Philippe start with it.

Philippe Fouquart:Thank you Wolf-Ulrich. I'm Philippe Fouquart. I'm with Orange.

Khalid Samara: Khalid Samara, Middle East Network Operator Group.

Olivier Muron: Olivier Muron, Orange.

(Martha Debill): (Martha Debill), (Edel).

(Alain Vedehoy): (Alain Vedehoy), (Todo).

(Papala Nowoa): (Papala Nowoa), (Intellui).

Tony Harris: Tony Harris, CABASE Argentina.

Thomas Rickert: Thomas Rickert, Eco Internet Industry Association.

Wolf-Ulrich Knoben: Wolf-Ulrich Knoben, ISPCP Chair.

(Karl Steffen): (Karl Steffen), Eco Internet Association.

Christian Dawson:Christian Dawson, i2Coalition.

(Sterling Stano): (Sterling Stano), CABASE Argentina.

Bastiaan Goslings: Bastiaan Goslings, AMSIX, the Amsterdam Internet Exchange.

Tony Holmes: Tony Holmes, Vice Chair, ISPCP, BT.

Wolf-Ulrich Knoben: Thank you. And we have some guests in the background so if you could just step forward and say your name yes.

(Andy Pitts): (Andy Pitts), BT.

(Mohamed Sadif): (Mohamed Sadif) from FlameHosting.

Ram Krishna: My name is Ram Krishna. I am also a member of the ISPCP from Nepal.

(Jesus): Good afternoon. And (Jesus) from Brazil.

(Walid Hunt): (Walid Hunt) from FlameHosting.

(Zeller Sees): (Zeller Sees), FlameHosting.

Wolf-Ulrich Knoben: Thank you very much for the introductions. We have still seats available. If you like you can join us at the table as well. We have a fully packed agenda today and also we are supposed to have around three hours available for today's meeting.

But we have some items to cover so any – we could be flexible in covering the agenda as well. First, well I would like to ask if you are satisfied with the busy agenda, if you have any comments to the agenda, additions or so. Anything?

Nothing. Thank you very much. Formally I would like to ask if there are any amendment of Statements of Interest you may disclose here. I'm not sure whether we have newcomers, you know, who are not so – that familiar with that.

A Statement of Interest is just a formality here in all ICANN meetings well to disclose, you know, where we come from and that everybody knows well this is a real person, you know, who is participating and on which behalf he's participating. But maybe Tony?

Tony Holmes: Just a quick addition to the agenda. A number of us were in the identifiers workshop this morning and the fact that it was this group that stimulated some of that action – but if I could just have maybe two or three minutes at the end and maybe others who were there can join in just to bring everyone up to date.

(Walid Hunt): Well – me – I guess I want to comment how the community mentor program just at the end and kind of this point today.

Wolf-Ulrich Knoben: Okay thank you very much. So we have to think about how we do that. I would, you know, I'm – and I just put something on the AoB in the end. I do not hope that we really meet, you know, until 6:30 here before we start with the AoB.

So – but I've taken to consideration these two requirements so that we can talk about and have an exchange on the two topics as well. Thanks very much.

We should be a little bit flexible with regards with the agenda. My question is that first do we have participation from abroad? Is there somebody on the Adobe Connect of – from abroad? Do we have any?

Tony Harris: I – there's a call anyways.

Wolf-Ulrich Knoben: There's not.

Tony Harris: I put it there.

Wolf-Ulrich Knoben: So maybe if there are then we'll give notice – put notices. We – what I do – we are interested with the agenda as Thomas Rickert is available today, and so we have two topics which we would like to cover with him together.

The one is the GDPR and the other one is the – an update on what's going on within the CCWG accountability and what is phases of it. And it would be nice, you know, following the discussions we – but which have already been taken with – on various opportunities within the ICANN meeting with times on GDPR that we may then concentrate at first.

At first it would be good to get some more insight in the backgrounds of the – with regard to GDPR and I know Thomas is a – an expert on this, you know, and I think that would help us to understand some of these processes and some of the impacts now, and not only on us but well it may be related to us and that would be helpful.

And then maybe if we could find out – to find out really and focus on the impacts with regards to our own business, to the ISPs, how we will be impacted by the GDPR.

That would be good to have well and I'm happy well to have you here Thomas. And afterwards we will go to the next item, which is then CCWG in order that we have a continuity with him together and can then say goodbye to you after that and then start with our – the rest of our agenda.

So thanks very much. Happy to welcome you Thomas and happy to hear from you and let's dive into the item.

Thomas Rickert: Thanks very much Wolf-Ulrich and hello to all of you both in the room as well as remotely. Now if you talk about GDPR now then about CCWG it pretty much looks like I'm jack-of-all-trades.

And what most people don't know – the second half of that is master of none so I would try to do my best to cover both topics. Obviously Wolf-Ulrich wanted to take advantage of the fact that I'm with you and I have been discussing GDRP – GDPR quite a bit over the last couple of weeks and months.

But I should clarify that the slide deck that you see here was one that I presented for a different purpose, so just to make growers abundantly clear I am here in my capacity as representative of the Eco Association.

I just didn't have the time because this was sort of a last minute arrangement that I would cover GDPR as well, so I used the slide deck that I'm using from my law firm usually.

So don't – let's not get that confused. I will get that on Eco's corporate identity if you want to further distribute this. And I should also say – and the two gentlemen sitting to my left might be – might've been too shy for this but I should say that Eco and i2C are under an MOU for quite a while.

But we thought that our organizations are working quite complementary, and in order to strengthen our services to members on both sides of the Atlantic we have now intensified our collaboration and come up – came up with a new vendored offering for our members.

But if you are interested in that -- that's what we call the Global MVP Program -- then please do reach out to one of us. Now I would suggest that in the roughly 45 minutes that we have that we devote something in the area of 30 minutes to GDPR, which is going to be a quite tough ride for you, and then for the remainder of the time that we're going to discuss CCWG.

But for CCWG since I've been at the ISPCP last time to give you an update about what we are planning to do, I'm going to focus on the latest news only. So GDPR is the General Data Protection Regulation and that's going to enter into force next May on May 25.

And it's a regulation by the Europe – in the European Union and the important thing for us is that this regulation is, number one, applicable immediately and it is also relevant to players that are not in the EU, right.

So even if you are not established in the EU you need to be cognizant of the GDPR. Since this is a regulation opposite to a directive it is immediately applicable.

You know, so many of you will know that the European Parliament adopts directives and these directives have to – have a little bit translated into national law and that usually takes quite a while.

But in this instance since it's a regulation it's directly applicable, so as of May 25 you need to be fully compliant with that regulation. Okay so the goals of the GDPR are the protection of natural persons and their personal data in particular.

And it shall give European citizens a better control over their personal data and regulate how controllers may use personal data. The same time it shall facilitate the flow of information throughout Europe and abroad.

So – now some of the main things and we should dwell on those for a few seconds are increased transparency requirements, increased documentation information proof requirements.

So this is something that applies to you regardless of what business you are, so you need to be transparent about what data you collect, what you're using with that data, to whom you pass that data on to your customers.

So some of you will need to revise their contracts and their information when onboarding new customers, because these are transparency requirements that are augmented or enhanced to what we had so far.

Then we see increased data security requirements. I'll get back to that later. We have additional accountability requirements and what's new here is that there's a duty to report breaches, both internal breaches as well as external issues.

You know, so even if let's say a staff member makes a mistake and data is let's say erased where it shouldn't be or disclosed where it shouldn't be, you might need to notify the authorities of that breach.

Or – and in certain cases you might need to inform the data subjects concerned about the breach. Same with the prior full let's say of cases where your network has been infiltrated and where there are attacks from the outside, right.

And this is something that - most companies don't want publicity to go along with breaches but that's actually something that might happen if you are subject – or if you are the object of or the victim of a data glitch.

Then what's new is the right to be forgotten or the right to erasure, and that means that you can request as a customer that your data is being removed and that your, you know, your track is entirely erased on the – from the databases of the company.

Certainly that does not go as far as deleting data that you are legally obliged to keep. So let's say if you're invoicing your customer, you have bookkeeping and archiving requirements, those would not be superseded by that.

But you would need - let's say if you're a social media or a social network operator you would need to remove all traces of that customer from that system.

Then we have the right to data portability so it must be made easy for data subjects to change providers so they can basically say, "Give that data to me. I want to change providers."

And so far, you know, these information requests at times have been honored by the operators by printing kilos of paper and hand that over to customers. That will not further be possible so you need to hand it over in an electronic format.

And many companies that expect a lot of customer flow are actually creating APIs whereby the data can be handed over. Then we have privacy by default, which is also an interesting concept.

And, you know, if you're doing business into Europe you need to bear that in mind and that basically means that you can't pre-tick boxes anymore. "I consent to this or I like this. I want your newsletter," and what have you.

But you need to have privacy settings by default. Let's use the analogy of a social network again. So you can't put everything as a standard on maximum disclosure or publication of data, but it needs to be quite restrictive and then it's up to the customer to review more and change settings.

Same with privacy by design. If you have designed your technical systems to capture as much information as you can, that will no longer be legal so you need to design into your products the capability of honoring the principle of data minimization.

You know, so those are some of the things that will be – will have significant weight, and then let's look into what's being protected by this regulation. It's personal data, personally identifiable data of natural persons, not by legal persons and that can be a lot of things.

It can be everything that can be related back to a natural person directly or indirectly so it can be name, address, identification number, location number and many, many more things.

Can be IP addresses static or dynamic, right, so you need to be cautious keeping log files because if you are not – if you don't have a legal basis for keeping that then that data processing might be illegal.

One word about legal persons. As I said this regulation protects the data of natural persons, but even if you have a company name that includes the name of a natural person that allows that – a link to the natural person, that might be considered PII, personally identifiable information.

Again so in case of my law firm that would be Rickert Rechtsanwaltsgesellschaft, Rickert Law Firm. That could be PII, right, so don't just rely on the company field and say, "Okay everything that – that's just self-identified as company data is per se not protected under GDPR."

The opposite is the true – is the truth. You need to look into that carefully as well. Now processing of data – a lot of folks think that processing of data are just a few things like collecting and then you do whatever you want with them and then potentially erasure.

Processing of data is a lot of things. That is collection, recording, organization structuring, storage, adapting, adaption (sic), alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

So pretty much everything that you can do to a data element through its lifecycle is processing. Then the concept that you should be familiarized with is the concept of data controller versus the data processor.

So you can read that later but the data controller determines the purpose of collection and processing, so the controller says what data shall be collected and how it's going to be used and to whom it shall be transferred.

And the data controller is responsible for following certain requirements for data protection and data security, so the onus is on that entity to make sure that the data is respecting the rights of the data subject. The data processor – I think this doesn't work.

((Crosstalk))

Thomas Rickert: I've been trying it over and over again but it doesn't – needs to specify what he does on behalf of the controller, and the data processor is also responsible for treating data confidentially and securely.

Now in the – you have this consideration of data controller and data processor, and I think particularly when it comes to the public forum and other discussions throughout the week on GDPR you will hear a lot of talk about ICANN's role as a data controller or not.

And so far ICANN has been in full denial that they are the controller because they said, "Well we are actually only requiring the Contracted Parties to do certain things because the community tells us to do so," right.

But if you look at what ICANN is doing, ICANN has the WHOIS specification. These are the data elements. They have the data retention specification for registrars specifying exactly what needs to be collected and how long it shall be retained, right, and they enforce if the contracts are breached.

And I think this by definition pretty much is everything that you need to be a data controller. But ICANN can be a data controller but a registrar – he sets up an account for a customer for invoicing purposes, so the registrar might be a data controller for a certain set of data elements.

So, you know, you – in one contractual relationship you can have different scenarios. You can have a controller/processor relationship. You can have a co-controller relationship.

You can have a joint controller relationship and all the like for different data elements and also for different purposes. So the registry might need certain data to register a domain name and in that instance I'm just speculating here and that – for that data element may well be that the registrar is only the data processor.

But for a different purpose than registering the domain name, i.e., for invoicing purposes, the registrar might be the controller for that data element. You know, so that needs to be looked at in a very differentiated manner.

And it result in joint liability and that is new. So far the data processor could lean back and say, "Okay the – all the responsibility and the risk is with the data controller."

This is henceforth now no longer true but actually they are both responsible. They are both subject to liability and sanctions so an aggrieved data subject can go to both the controller as well as through the – to the processor for relief.

Principles are – of processing data needs to be processed lawfully, fairly and in a transparent manner. And I mentioned earlier…

Wolf-Ulrich Knoben: (Unintelligible) been some questions in between, you know, for understanding.

Thomas Rickert: Are there any questions? Sure.

((Crosstalk))

Thomas Rickert: I don't see the Adobe room so…

Wolf-Ulrich Knoben: Yes okay.

Bastiaan Goslings: Yes thank you. Sorry for interrupting. It's Bastiaan speaking. Just to confirm so I understand correctly, right, you referred to the example of registrars, registries and ICANN itself.

From your perspective if I understand correctly ICANN would then - also can be considered a controller. But for the same data set or the same data field for instance, you cannot have simultaneously more than one controller, right?

Thomas Rickert: You can. You can.

Bastiaan Goslings: For the same – okay.

Thomas Rickert: Data element. Yes.

Bastiaan Goslings: Okay because I understood - like this is my conclusions. That's why I'm checking from - your example is that you refer to ICANN, why ICANN could be considered a controller and then you referred to the registrar and then you went to the – on to the billing information. There seems to be another set of data that they then would be…

Thomas Rickert: So it can be, you know, they can be partially congruent…

Bastiaan Goslings: Okay.

Thomas Rickert: …business data elements. You know, let's say then the name of the registrant might be needed to register the domain name by the, you know, let's say the registry wants to get that data yes.

So they need it for the purpose of registering the domain name, but the registry doesn't invoice the customer but the registrar does or the reseller does.

So the reseller might be data controller for that data element for invoicing purposes because they, you know, they have their own idea of why they need the data so it needs to be looked at in a very differentiated manner. Question?

Christian Dawson: Hi. Did – were you in the session with – where we spoke to the board about GDPR?

Thomas Rickert: No.

Christian Dawson: Okay I wanted to fill you in on one thing that is actually relevant to the specific things you've just gone over, because we addressed – we tried to pin down Goran on – to the - ICANN's role as a data controller.

And we went further because we wanted them to describe not only their role as a data controller, but to describe their role as the contract holder for the escrow account that Iron Mountain has.

So basically when a registrar registers a domain name they collect a whole bunch of data and then they send it to an escrow provider. That escrow provider is Iron Mountain.

That's a contract with ICANN. Iron Mountain then provides a subset of that data as necessary to the registry in order to operate the whole domain name mechanism on both sides.

So we said, "We need to fully understand your role as a data controller and your role or Iron Mountain's role as your contractee as the data processor." And Goran said, "We may very well determine that we are a data controller."

I'm being very careful about not using those words right now because I don't want to put anybody including this community in jeopardy before we have the final determination legally that we are, and if we are we will ensure that we take the responsibility of that. So that was a good…

Thomas Rickert: Yes.

Christian Dawson: …outcome I think.

Thomas Rickert: Yes. I have a slide later in this slide deck where I speak about if the role – escrow agent and all the various players that we need to take into consideration.

But, you know, that's – I should probably only say that ICANN does not necessarily need to wait for somebody else to tell them that they are the controller.

You can determine that by contract and I think it would hurt the community a great deal if ICANN were accountable and brave enough to say, "Okay we want certain data elements to be collected and processed," and therefore we sort of voluntary assume controllership for these data elements which didn't happen so far.

Okay so you need to have a legitimate purpose for processing data and if let's say you get the data for the purpose – from a customer for the purpose of shipping a book to a customer that has ordered a book with you, you can't use that data and publish it worldwide, right.

So that would be a different purpose. You must – you also must not transfer it on to somebody else if the purpose of processing is just delivery of the book in this case, and therefore you can't make up additional purposes that go beyond what's legitimately required, right.

And that's the concept of purpose limitation and those in the ICANN world who said, "Well we just need to define a purpose that is broad enough and wide enough so that we can keep on going with our current system," that just doesn't work.

You need to have a purpose for every processing step and you need to be able to justify that purpose. Okay so we are going to speed up here a little bit. So you – there needs to be lawfulness of processing.

And I would just like to highlight two of those options, one of which is B, the processing which is necessary for the performance of a contract. You are entitled to collect and use data that you need to fulfill the contract.

So if – on the online bookshelf and if the customer wants to get a book from me, and then I certainly need the name and address and billing details so that I can send an invoice and ship the book, right.

And for that I would not need customer consent because that is inevitably required to conduct the contract. If I want to go above and beyond that then for each – every additional processing step or each additional data element that I want to obtain I would need consent.

And consent is enshrined in A. Consent needs to, you know, person can give consent to the processing of his or her personal data for one or more specific purposes.

You need – so you need consent for each and every processing that goes above and beyond what's legally required to fulfill the contract. So I think we could, you know, we can go back to more detail on this but I just – I'm – I'll try to keep this to the minimum.

Few words about consent. Yes consent is a way of obtaining the customer's green light to process and collect data, but particularly in the domain world you need to bear a few things in mind.

Number one, the controller needs to be able to demonstrate that the data subject has actually consented so you need to document that. Then the subject – data subject consent must be based on an informed decision so you need to be – need to clearly identify what's being done with the data, for what purposes, to whom it's transferred.

That all needs to be displayed and if you don't do a good job with that, then the consent is invalid and that's quite a challenge for Contracted Parties, right.

I should say that the registrars have the requirement in the RAA to get the user's valid consent, but nobody really cares about that at the moment. And at the moment consent is – if – and is void for most of the cases, right.

So this is something that you need to do a good job. You know, you need to be very transparent in your information. And then another hurdle is that consent can be withdrawn at any time without giving any reason.

Now we have a decentralized storage architecture in the domain world, you know, so you need to make sure that you get the data removed from the registry, registrar, (EB) Europe, from escrow agent and if you have resellers in the mix it would need to go be removed from all reseller hubs.

That's quite a challenge, right. And then consent must be given freely and there's a prohibition of coupling. Now what does that mean? If you say, "I will only give you a domain name if you consent to your publication of the WHOIS in the public WHOIS data – of the data in the public WHOIS database."

Then one could argue that that consent is not freely given because you will decline the domain registration if the customer doesn't agree to this handling of the data.

Now you might say, "Thomas this is speculating over things." But this is exactly happening at the moment with – in the Netherlands where, you know, we have some hiccups with the data protection of ITs who have said that FRL is, you know, they couldn't handle the things they previously did.

You know, so these are real-time – real-life examples and the lawyer of the FRL registry has written to ICANN and complained that, you know, the consent as required by the RAA is null and void because it is linked to excessive data processing.

Then controllers - and, you know, this will apply to all the (GS) companies. You need to create a record of processing activity. You need to detail each and every process in your company relating to personal identifiable data, and there are further requirements with it.

I'm not going to – into details here but, you know, this is quite a challenge if you don't have such documentation yet. There's a comparable thing for data processors and for the sake of keeping time I'm not going to go through that.

You need to set up a data security management system, i.e., a system where – which contains the record of processing activities, but then you also need to have processes in place for data breaches.

You need to have processes in place for changes in your setup, i.e., when you are onboarding new contractors or new services, you know, so that you have a good process through changes to your data protection setup.

Then you need to have a rights management system. Not all staff must get access to all data that you have, right, so certain data must only be visible for certain types of staff or groups in your company and certain data needs to be blocked from their access, and all that is regulated in this management system.

Okay few words on to whom GDPR is applicable. If you are in Europe in the EU you need to be compliant. If you're outside the EU you need to be compliant if you have customers in the EU.

If this is just occasional then you have an exemption from that requirement, but if you are offering your services into the EU chances are very good that data processing is not only occasional and then you need to be compliant.

And then also you need to have a representative in the EU in one of the companies where at least one of your customer resides. And if you fail to appoint a representative that is subject to up to 10 million euros fine or up to 2 million euros of annual global turnover so that's quite, quite serious, right.

So it is applicable if you fulfill these requirements. I mentioned the 10 million euros as the – the 10 million euros fine. Actually the highest fines would be 20 million euros or 4% of the global annual turnover, so that's quite substantial and there are a lot of companies in this arena who are more afraid of the 4% than of the 20 million euros.

How to become compliant. So I'm going to go through this very, you know, not to every slide because that's going to take too long. So you need to check whether GDPR is applicable to you.

Then you need to establish what processes you have. We've touched upon that a little bit earlier. Then you need to conduct a gap analysis of what of these processes are not compliant, and you would look at what processes would be – would pose a great risk to a – customers and what – which of those risks have a high probability of becoming true.

So you go from high risk to high probability to low risk/low probability when you're trying to fix these things. So how would you determine whether your handling of data is legit?

So first of all you would determine whether personally identifiable data is present. Then you need to take a look at the origin of data. Is that data that you have collected directly from the data subject, or did you get it from third party in which case and in both the case – which cases there would be different legal implications?

Then you need to check whether the purpose of that processing is – holds water and whether that's a legitimate purpose. You need to look at who gets access to that data, access internal/external and to whom you transfer that.

So if you want to ship data from the EU to the U.S., you know, do you have EU standard clauses in place that would – or binding corporate rules that would justify the data transfer, or are there appropriate agreements or consents in place for shipping the data to other third countries?

Then you need to take a look at where the data is stored and whether that storage is legitimate, and you need to take a look at the retention period for that data because you must not keep data longer than required or longer than legally – than you have a legal basis for.

So the – once we have the record of processing activities ready and once everything has been implemented, you have your data security management system ready which is a – sort of a dashboard type thing as I mentioned earlier where other processes and other procedures are laid down, so that should be the central source for everyone to look at and understand exactly what data is – how data is handled and how you – how your internal processes are.

And in fact if some – if a data protection authority wants they can go to you or in case you're outside the EU they can go to your representative and ask for that information.

So you can't just start collecting that information and aggregating those documents when you are asked, but they need to be ready for the - proceeding to the authorities if need be.

Okay in the G world -- and I'm going to end this very soon -- we have the complexity that - we have the terms resellers, registrars, registries. ICANN - we have the emergency backend operator in case of registry failure and we have the escrow agent.

And a lot of folks are only talking about WHOIS these days but WHOIS is just part of the issue. You also have, you know, you need to check whether all data elements can be legitimately collected as we have at the moment, and chances are slim that this is sustainable.

I know of no one who is using the billing contact as publicized in the WHOIS. Registrar set up accounts. They send invoices to account holders. They don't use the WHOIS data for that purpose, so that might in itself be excessive collection.

And then, you know, the fact that you may legitimately collect your customer's data is not a good enough purpose for revealing that data and disclosing it in – publicly in WHOIS.

So, you know, there will likely be a lot of change. Also if a registry fails at the moment ICANN can request the escrow agent to pass on that data to EBERO, and if EBERO is not running in compliance with GDPR the system is broken.

Or if a registrar fails then ICANN can request the escrow agent to pass on that data to a gaming registrar, and if that registrar is not fully compliant the system is broken.

So we need to take a look at all those aspects including data retention and many more. So some say that law enforcement must get access to that data and that, you know, preventing fraud and all that would be good reasons to maintain a public WHOIS.

The legal opinions that ICANN got so far say the opposite. They say if law enforcement wants to get access to that data there needs to be a legal basis. And we have to police their access in the EU that offers the possibility of establishing legal instruments to get access to that data.

Even for private companies, security companies, spam fighters and the like – only has the – have the European lawmakers never availed themselves of that opportunity, right.

And the question therefore is shall the registries and registrars take the risk of being sanctioned to keep open that inventory of data, or should we rather be compliant and ask the European lawmakers to come up with the instruments so that their investigations are not hampered by new approaches that might need to be taken, right?

So let's – that's something that we need to be very clear about. On top of that privacy services have not prevented all sorts of investigations and, you know, reveal upon requests can be – still be an option opposite to public WHOIS per se.

So I think we're – I only want to say two or three more words about additional requirements beyond May 2018, because it's not good enough for you to just have a – have everything in place.

On an ongoing basis you might need a data protection officer. You can have an internal person or an external person to do that for you, and that person advises the company on how to deal with privacy basically.

Then you need to keep your data security management system up to date, right, so you can't let it sit there but it actually needs to be a vivid document for bigger companies that's software-based and that needs to be kept updated.

You need to appoint a representative in the EU if you are abroad. You need to think about incident response. How do you handle data breaches? And you can liaise with – consult in that regard who are standing by to help you how to communicate to whom in that regard.

And you need to train your staff. If you don't train your staff nobody really knows how to go about with this so that's a requirement as well. So I think if you're doing all that then you can say mission accomplished but until then still a while to go.

And discussions with ICANN are going to be quite tough I guess because so far ICANN hasn't been very cooperative on these things so that, you know, it's going to be tense for the Contracted Parties to be compliant in 2000 – May 2018.

And what's crystallizing now at the moment is that ICANN will likely work on this as a priority contractual compliance matter, not involving the whole community.

But then certainly the question is how do you deal with that beyond this interim phase? So there needs to be some policymaking subsequently or in parallel to this contractual compliance handling.

So if you are expecting an answer, you know, what are we going to do if all the WHOIS goes dark on May 25, question is will ICANN forbear its right to enforce the contracts on a temporary basis or the like?

And I think that the Contracted Parties would be very grateful if the ISPCP would support interim solutions that would prevent them from getting breach notices from ICANN.

I think I should stop there and ask whether there are questions? It's been a tough ride, right.

Wolf-Ulrich Knoben: Yes. Thanks very much Thomas for this lesson. Well it's helpful and educatory for people here I think so – well to learn, you know, what is really the background and what we have to expect and what are the different aspects here and we have – we may have to take into consideration and in the future.

So the – I think as these discussion here over the ICANN meeting is going on this morning – so we have heard, you know, as Christian was first putting this question with regards to the whole of ICANN towards Goran.

So maybe - it seems to me that ICANN is a little bit - well it's a little bit diligent or - well or cautious let me say about that. So I understood Goran that he would like to have legal advice on that, you know, on whether ICANN has a role to be compliant yes in this regard and then in which ways, you know, and a second steps – step as well.

And as long as he doesn't have solid ground on that – so he doesn't like to give any – well doesn't like to show any support and any reaction, you know, of that so those are impressions this morning about that.

But nevertheless – so I think for us it's very important to know and to understand, you know, this – whatever is coming on and how we as ISPs might be – have big exchanges or in which sense who are as an exchange, you know, just – let me say just transporting data yes rather than processing data or in which sense or are we touched with – by this and in which direction we are touched by this depending on how we deal with the data which are – which we are transporting.

And that's up to us now to clarify internally so – really and then to take measures and see how it works. I'm sure you know that for the lawyers it will be a good business in future.

So – and anyway, you know, so either to get advice, to do – to get – give us advice or to accompany us to – going to court or so on. And so this is a really broad issue and broad ground, you know, of several types of issues.

So if there are questions and there may be questions. Yes Philippe so please start these questions and maybe then comments on…

Philippe Fouquart: Thank you. I don't know if it's a question really but to you – your first point and the role of or the responsibilities of ICANN in that respect, I remember that in a meeting on GDPR internally not related to DNS or – but in general internally within Orange it was summarized pretty much as you need to know what you've got and you need to know what you do with it in terms of personal data.

The concern I have as it relates to ICANN is that it – I can see that there is – they're weary – wary of having legal advice on this and that's good on one hand.

But it's also a matter of where you start from and it – when you put that in light of the response that was given yesterday during the public forum on the background screening files and data that was collected during the gTLD application phase, I'm concerned because if on that quite important question there's no one that is in a position to answer that, I think it's going to be a long ride to comply with it.

It – that's just an observation but I think there's the process that is being followed and I think there should be legal advice and that's good, but there's also the current practice and we're all there.

I mean, we've got data everywhere, you know, but I think that we're not – certainly not in a good shape to be compliant by May next year.

Wolf-Ulrich Knoben: Any further comment or question? Please the colleague from BT, British Telecom.

(Andy Pitts): Yes just to follow on really, I mean, you know, it's only seven months away to be compliant. There's – and there's a – I know internally within BT we've had teams looking at this for, you know, some time now.

So as I say it's all coming very quick and I'd just like to thank Thomas for the presentation. That was – that's very good certainly. Yes. There's a few points in there that I didn't quite realize that come under that so thanks for that.

Thomas Rickert: Much appreciate it and I – let me just say that, you know, GDPR looks like an overwhelming task but your comment was spot on and that's what I tried to say when you establish the status quo.

Look a lot of you have ISO certifications or other documentations of processes. That has a great deal, right, so build on what you have, understand what data you have and how you deal with the data and then either internally or with external advice you analyze what you have and you identify the gaps.

You know, so, you know, it's manageable. It's an iterative process but Wolf-Ulrich when you said, "We need to check how we deal with this as ISPs even if you didn't have any customer related personal identifiable data, you still have employees."

So everyone needs to look at those processes. You know, what's employee data? Who gets access to that? How are paychecks being treated and stuff like that? You know, how do you deal with data of your suppliers, you know, let alone the customers?

So there are a lot of things that every company needs to look into. And, you know, the contracted parties in this game are the unfortunate situations that they have to do all the domain related stuff on top of it.

And with respect to that, they're additionally in the uncomfortable situation that law enforcement, government, IP lawyers are all relying on a resource called WHOIS for their investigations that was always public and, in my view, was never legally public, right?

And it's always difficult to turn back the clock. So we're now - many in the community are in the mindset of, okay, how do we do tweaks to WHOIS so that we can keep it? We should reverse the thinking. Bear in mind the principle of data minimization. We should take a look at this like what data do I need in order to register a domain name?

And then there is not much left, right, so - and in terms of data for investigation purposes, who would assume that you can just - that you would force a telephone company to publicize mobile phone numbers with (all) customers for details including email address, telephone, fax and what have you?

So that doesn't happen in any other industry, but in the domain name industry it's taken for granted. Why?

Man1: Okay, thanks, Thomas. Very last question, then, from (Christian) but before we - and we have to move forward because for the next one - so I expect all the other guests from ICANN here.

Christian Dawson: Very brief. I wanted to - because I agree with everything you said. All I want to do is say - put in a plug for involvement in the next gen RDS PDP working group which I am in and Jennifer Taylor is also in.

That is where we are attempting to build a replacement for WHOIS that does exactly that. We're attempting to build a data minimization model and a potentially gated system that is going to be in compliance with local law.

(Goran), today in his conversation with us, did note that they are well aware that ICANN rules cannot trump local law. It's great to hear that from him again even though he twisted it the first time. He came back and he corrected it.

But not everybody in that group agrees that that's the way we need to have it but it is the way we need to head it and the more help that we can get in getting us there quickly the quicker we are going to have a working WHOIS which may go away after May 25 for a little while until we fix this problem as a community.

Man1: (Unintelligible). Yes, very quick.

Woman1: Yes, and (unintelligible) because it's very complicated if I actually want to explain it so widely. It could take a very long time. And it's just that a big chunk of the data actually possessed by ISPs and (unintelligible) service providers is actually not subject to the GDPR but to another more restricted piece of legislation which is the privacy directive also now being reviewed.

And actually - so the biggest chunk of the data provided - possessed by telephone operators, traffic indication data, is not subject to this but to another one.

And I was wondering if that has any implications in the exchanges of data with all the other stakeholders in ICANN, if anyone is looking at that.

(Raul): I think that's a good point and I've obviously focused on general requirements and requirements for ICANN players, let's say but particularly since we have companies that are offering different services.

So they are (IFCs) plus they're offering domain names and stuff, I think it would be good for the ISPCP to raise awareness for this additional dimension of data protection with the (privacy) directive that's coincidently going to come up. You know, so I think that's a very good point.

Man1: Yes, thanks very much and - (Raul). So let's move over to the next one. And do we have already (Brian Shilling) here in the room? No, not yet, (just) more ICANN, because he would come then to the next point. Thomas, well, I have to call you for the next - to entertain us.

Thomas Rickert: Happy to.

((Crosstalk))

Thomas Rickert: Sure. Well, as you know, I'm one of the CCWG co-chairs and we had a face-to-face meeting last Friday. And what I can say is that we are on track, so basically this is the timeline.

As you might remember, we have asked for one extension in terms of budget and time until next June. And in order to make the June date next year happen, we need to wrap up all the substantive work in the sub-teams very soon.

You might say this is more than half a year to go, and therefore, why are you rushing so much? But actually the process of wrapping this up is quite complex and we're going to have a visualization of that in a moment.

So I'm going to show that to you in a moment. This is the completion status of the sub-teams that we have. So everything is on track. Some are a little bit further.

Others are right on track, but all sub-teams, you know, that we've structured our work with - sub-teams that are working on different subject matter, it's all on track. And that's very good news.

So this is the table of the completion status of the various sub-teams so those in the - on the other side of the slides are either versatility staff accountability, ombudsman and jurisdiction - have gone through successful second readings.

You know, there should be a tick on the jurisdiction thing. We're just missing here. And those are going to go into public comment, right, so there's an opportunity for you to review the reports of these sub-teams and chime in.

And for the groups on - so AC accountability, human rights and transparency - let me check this - we had public comments and just had minor additions, you know, minor changes that were merely cosmetic.

So all in all, we're in good shape. And Wolf-Ulrich asked me to focus on the things where PCP is required. And this is the slide where this becomes particularly relevant.

You need to make yourself heard when it comes to public comments for the individual reports, you know, so you see in orange, this is no promotion for the (police) around the table.

In orange, you have the sub-team reports which are for the public comment periods that are still open. After that, we're going to put all the sub-team reports in one package that's going to be our big final report and were going to have another public comment period for the whole package.

And that is limited to incongruences between the various packages because it may well be, let's say that, the jurisdiction group to something that is in conflict with the diversity recommendations, right.

But there, we're just looking at inconsistencies, so check the report for inconsistencies. If people, which I think are quite likely, tried to get a second bite of the apple and then try to introduce new changes to the sub-teams, substantive reports, we will not honor that but we will collect that in that can then go into another ATRT or other review that's going to take place over time, right.

And then once we have this final report gone through public comment, (done and dusted), approved by the CCWG plenary you will be asked to chime in again because then we will seek approval from the chattering organizations and the GNSO is one of the chartering organizations of this cross community effort.

And we hope that you will just represent this and say, okay, we've got enough public reviews of the individual reports and the aggregated report, so we hope that you will help us in getting the approval from the GNSO and the other chartering organizations.

Then this will go to the board and the board will then need to approve it. And we've already had one instance where the board said, well, on the transparency recommendations, you know, we might have an issue with open contracting and stuff like that because it might bring the cost up of our procurement processes.

And then (Robert Turk), for the transparency group, said, "Well, that's a good point that you make, only that it's wrong because studies in various countries have shown that by using open contracting, costs have gone down by 30% average," right.

And I then asked the board representative, well, was priced really concerned that you had? And he said, "Well, I don't really know." So the board might have last-minute things as in work stream one where they might wish to tweak things to their benefit.

And I think we, as a community, need to stand firm and pressure the board not to try to introduce late changes or requests for changes. If the board approval is refused, we will need to go into overtime and I think we don't want to do that, right.

So let's pressure the board when we talk to the board - let's pressure them to take a look at things now so that they can't hold up the train for overall approval.

And, you know, I'm not sure whether you are interested in updates on the individual topics. I would only pick one and use two or three sentences and that I will end my presentation and that is on jurisdiction.

There will be another session on jurisdiction on Thursday. And what you should know is that there are some country representatives who are unhappy with the results of the jurisdiction work.

And there are both procedural, as well as substantive allegations that are floating around all the time. What I can say is, that our group has look at all sorts of issues that have been identified.

In our group has diligently discussed all those issues, not at the level of detail that we would have loved to, but in the time given, questions such as community and others have been discussed.

There are those who would have loved to make ICANN an immune organization such as international - intergovernmental organizations. You can't sue them, right.

And they proposed this but these proposals didn't really get traction because people said, well, community is the enemy of accountability because if we can't take you to court, you know, we can't really hold you responsible for your doings.

And, therefore, it's not that these requests that have been brought over constantly and over and over again have been ignored. It's just that these requests haven't received sufficient traction.

I appreciate that we could have gone - made more recommendations but we did what we could do on time and I'm sure that accountability discussions with respect to jurisdiction are not over when work stream two is over.

But we came up with two recommendations that are actually great, one of which deals with (OFAC). That's the office in the US that has sanctioned lists of countries and individuals.

And at the moment, ICANN tries to get an (OFAC) license to enter into a register - registry or registrar agreement with parties from sanctioned countries but they're not obliged to do so.

And with our recommendations, we're forcing ICANN to use best efforts to get those licenses so that DNS can only be - also be used in those sanctioned countries.

Second recommendation is on contracts; While ICANN's contracts to not have a choice of law provision, these are clearly US-based. I mean, you've read them, right? So there are legal concepts that we know from the US and we know that this is not the most inclusive way of offering global services.

So we know of a number of prospect gTLD applicants that have not gone forward with a client for gTLD because they didn't (unintelligible) in the contract and, therefore, we're recommending what we call a venue approach which means that ICANN doesn't have to offer contracts under every jurisdiction in the world but they should (have at) least one jurisdiction per ICANN world region.

So that goes closer to the applicants, closer to the contracting parties. And I think these are good suggestions so if you see me being on stage in two days in this session and if there are attempts to slaughter us, come to our rescue.

I think we haven't done everything wrong. Thank you so much and sorry for going into overtime but it was a good discussion to have, yes.

Man1: Okay, thanks, Thomas. As long as you can survive our meetings here that I'm sure you can survive other meetings as well. Thanks very much. So, for use, you know, I understood the importance should be here - is the public comment period, you know, which is going (to take place) directly after the meeting or the middle of November, so (unintelligible) the working plan.

So the question is, well, there are six work streams, I understand. You have six reports, you know, the charter, there were six.

((Crosstalk))

Man1: Oh, these ones. Okay.

Thomas Rickert: We have nine.

Man1: So you have nine reports to be commented.

Thomas Rickert: Some of them have already gone through public comment.

Man1: Oh, okay.

Thomas Rickert: Some will be - one public comment period I think on diversity is open right now so you can still comment on that. And I think two reports will be put out for public comment in the next couple of days.

Man1: Okay.

Thomas Rickert: And I should note that IRP IOT's implementation (offers IT) for the independent review process. That is in work stream two but that's not going to be finished in work stream two because that is a remnant of work stream one, different budget, different timelines. You know, so we have a topics that go into the final report of work stream one.

Man1: Okay, so as I understand, well, while going to the (sub-standards), with comments, it's - that's now the time, you know, to go on so - because afterwards, when it comes to the entire report that it's too late because the question of which part fits or doesn't it to the other or so - discussion.

So I have a question here to the - to ask, you know, our group. So then which one of these reports are essential for we would like to comment on, you know, we would like to comment on specifically as we did, you know, (unintelligible) we did come into some of these.

But which ones are really essential to do so? And then we should find out, well, who could be volunteered now to do so and just (get with them). I'm looking, you know, as I'm looking with regard to accountability, I like and I'm inclined to look towards (Mericom) at first.

You know, but then I hear it first, like, let's hear from (Christian) what he has in mind please.

Christian Dawson: I think of all of those the one that we need to be heavily involved in his (SOAC) accountability. I think that's clear.

Man1: With regard to the SOAC accountability.

Christian Dawson: Yes.

Man1: Okay, so you would like to start…

Christian Dawson: I'm happy to help with that but I mean, that directly plays into things regarding - that have direct relation to what it is we do as constituencies, so we should…

Man1: Yes, we had this public consultation already.

Christian Dawson: Great, so there we go. Can we - okay, that…

Man1: If I may add, I think we could really do with support for the jurisdiction report. I think the recommendations are great and, you know, if you could just say we like this - because there will be opposition.

You know, there are certain countries and certain individuals that would prefer to take ICANN out of the US, make ICANN and you know, what have you.

So that we can likewise tear down and rebuild it entirely. You know, so I think some positive messages or support for the jurisdiction recommendations would be appreciated. (Tony), please.

Tony Harris: Thanks. Well, first, Thomas, I think you've done a brilliant job on this. I'll just say that - really good to get this far - is it really - a really good achievement.

And I agree with (Christian)'s remark, I mean, the one that we should have: four was the accountability without a doubt. There are some things in there that are still struggle with.

But the question here - you mentioned, Thomas, jurisdiction. No I think there was a session here with the GAC and I wanted to get into that session. I couldn't. Can you say how that went, without discussion? Interested to know.

Thomas Rickert: I had the constituency meetings why wasn't there and I need to go to the transcript but it's - it was an opportunity for - you know, Brazil has fired a dissenting opinion that was supported by Argentina, Russia, China, Iran and maybe two or three others.

So I think they wanted to go on record with their opposition to this report. Brazil, primarily based on (unintelligible) expectations there so they get back to that (unintelligible) whenever this is being discussed.

So I think they understand that, you know, their proposal did not get close to being eligible for consent, but nonetheless, they want to make themselves heard.

And I guess this is also why we're seeing the request from the GAC to have this jurisdiction discussion on Thursday. You know, but you should come if you can because we will have some group members that I think will be quite outspoken in defending the process.

Tony Harris: Just a follow-up question on that. I mean, the rest of this has gone through really well but the fact that that is such a difficult one, jurisdiction, so off the record, is there any thought that they could really derail the time frame on this through other mechanisms because of the volume of noise that that's generating?

Thomas Rickert: the jurisdiction sub-group report has gone through two successful readings in our group. So our group has done its share. So we would heavily see changes to that if there are inconsistencies with other work packages.

There might be pressure from the GAC, although I think that even within the GAC, the views held on immunity and relocation are minority views, so I think there - we can't expect the formal objection from GAC or even GAC advice.

I spoke to government representatives who are in full support of these recommendations and who don't support a dissenting opinion. So to what extent this is going to stir up dust, I don't know.

I think it's important to bring all the arguments out in the public and this is why we had, I think, in total, a three-hour part of our face-to-face to allow for Brazil, India - and India's was not the government but it was an academic - to put all their concerns on record to inform future debates.

So we will take transcripts of the three-hour session where everyone could let off steam. We will add that as a transcript to our report. I think that's important.

But I don't see realistic chances for this to hold up the train. Just the opposite would be the case. If we were asking for immunity for ICANN, that would require legislative (actions), if I'm not mistaken, in the US and if we brought this to Washington, I think that could have unintended consequences.

Wolf-Ulrich Knoben: Okay, thanks very much, (Tony) and Thomas. Well, just a quick question now - if you could fix that right now, so who is going (now) just to take over some things of these reports, now to comment on that, it shouldn't be very detailed, you know.

If that comes to a close, well, okay, we are in agreement with that, that would be good. But we need somebody, you know, putting that together just briefly and giving a recommendation to the list, on the list, so that we can file it (well) and then afterwards to the public comment page.

So I wanted - (Tony), would that be (fine) or how are you thinking about that? I think also, (Martin), you are following the accountability group, as well. Is there something you are, let me say, in favor or would you just now recommend to us, well, that's okay. The work is done from our point of view.

I know in (former times) during the accountability discussion, you were really coming up several times here and saying, “Okay, we must comment in this and that way.” And it would like to take your advice in this direction.

(Martin): Well, thank you. Can I introduce you to a concept known as volunteer burnout? I mean, seriously, I’m still - personally I’m still engaged on work stream one follow through which is the IRP implementation of the (unintelligible) and I will be reporting back to you on that when we have that out for our second round of public comment.

As to these, I have a very spotty level of tracking, actually. The ones that I would - that I would personally say, is yes, I would certainly support what Thomas has asked for in the jurisdiction thing because politically, it’s just good to make it clear to the communities behind that and not support the dissenting opinion.

The other one that I have given at least some attention to briefly was the transparency one. And on that I think I’m slightly disappointed actually in some respects because one of the key elements that what was intended to do was not able to be achieved.

Now, that’s not to say that we should not support what there is, yes. Actually, you know, there’s a lot of good stuff in there. It is, however, one of the things that - one of the key things that actually caused that to be set up in the first place was the ambition to get more transparency in the - I forget what the term is now.

Perhaps Thomas can help me, but the document disclosure policy particularly in the context of IRP cases, but also otherwise. And that relates to the - I CANN’s exercise of the attorney-client privilege and to attempt to get a - some kind of workable principle standard that could be used so that the attorney-client privilege which still exists would not - would nonetheless, not always be pressed to its full degree by ICANN.

So this enables - the client disclosure documents that legally (unintelligible) hold is under attorney-client privilege. I'm afraid that was - that group was not able to reach a consensus in favor of something - in favor of a principal on that.

And I think that that - and certainly I would suggest that that would be something that we might regret, and as these things are reported onto the board's attention for implementation, we might say that we think that the board - that we would prefer that the board went further than the report does and look to see if - and (start) to identify a principal that could do more in that area.

That's one area that I do have some advice. But on some of the others, I'm afraid I can't help you.

Man1: No, thanks. That's great. Thank you very much. And, well, (unintelligible) how we can manage it. You know, I'm willing to take over something, well, also to put in (another action item) to give advice to because we have the knowledge.

I wonder whether now give another person could join me in this combined effort and then maybe…

Man2: Are we just talking about jurisdiction now or writing up (kind of) jurisdiction or are you talking about actually making a statement, drawing up a statement on implementation once this is passed?

So one we can wait on, I think. I think that what you want - what you want to smart and it's probably a few months away. And then one, I think we need to work on relatively soon but it's also - it also can be short.

So I would be happy to work with you collaboratively on a jurisdiction statement. It could be two paragraphs. And, (Malcolm), I think your point is well taken but the time for, I think, that is when we're actually in implementation or about to go into implementation.

Man: You will have the opportunity to consider that - not now. Yes, that's (unintelligible).

((Crosstalk))

Man: Yes.

(Malcolm): Yes, I agree. I think couple paragraphs just saying we support the jurisdiction thing is absolutely called for.

Man1: So, (Christian), may I ask you, any (concept) to the public for - public comment page, you know, request and (such), is it 30 days? Isn't it, Thomas, 30 days or 40 - I don't know how much - how many but - so and you've (given a draft), kind of a first draft, yes?

Christian Dawson: I'll absolutely do a first draft. That's not a problem. I also think, Thomas, that if you successfully helped lead us through a kind of work stream one and jurisdiction work stream two, I just can't believe it and I need to ask you to move over to next gen RDS next just so you can do the next impossible thing.

Man1: I think that's good so (at this chance) we'll be waiting for your first draft to - please leave us some time so that we have a time now to coordinate on that. You know, sometimes we have misunderstandings or we need some more clarification on that. (Tony), you had a comment on that? No.

So to wrap this up, thank you very much, Thomas. Very helpful. Anything we can then close this point. And immediately, before - I'd like to have a break but, no, let's just continue because we are behind schedule already.

Man: Thanks for having me. Thanks for your input.

Man1: Thank you very much. And we have (Roy Arends) here from ICANN staff and he's also limited in time to talk about the (case key) all over delay in which he started to talk - to discuss with the board this morning on CSG level. Hello, (Roy).

(Roy Arends): Hi. We do have slides for that done.

((Crosstalk))

Man1: Yes, I have - I think they were sent to (Andrea). Didn't she provide you with slides? Did you send it to (Zechariah and to Andrea)?

(Roy Arends: Yes.

Man1: As I implied, so otherwise I could…

(Roy Arends): I can get another (unintelligible).

Man1: So just check it. Anyway, just to give you - I don't know why - have you had a chance to participate in the meeting which we just had with the board? So we have filed also - not filed, a question, but a - let me see a supporting message, yes, from us, now towards the board and towards ICANN that we are supporting what the board decided at the end, you know, to delay the (case) because of the opinion that it's necessary, really, to delay that.

And that we are in support also to - you would like to help you in the future through our communication channels and our business relations we have to find a new date and to find the procedure in which way we could move this forward. Will you be able to start - well, I'm just wondering whether the presentation…

(Roy Arends): Well, I'll quickly get it over to my (unintelligible).

Man1: Yes, no problem. (Just start it).

(Roy Arends): I can actually do this without slides. Is that okay?

Man1: Yes. Yes.

(Roy Arends: Yes? And I - a reference I can send the slides, then, later if that's okay.

Man1: Yes, (we can do this is parallel), so.

(Roy Arends): Okay.

Man1: (Unintelligible).

(Roy Arends): I pinged (Brian) a few minutes ago. No response yet.

Man1: Okay.

(Roy Arends): Perfect, thank you. Would you like PDF, PowerPoint?

Man1: (PDF please).

END