**Public Sector Future podcast**

**Detail: Episode 22**

**Audio File: Public Sector Future\_EP22-Antonio Gameiro Marques**

**Portugal\_Reference.mp3**

**TRT: 23:20**

**Talent: Olivia Neal [host]**

**António Gameiro Marques, Rear Admiral National Security Authority, General Director [guest]**

**OLIVIA NEAL:** Hello and welcome to Public Sector Future. This is a show for anyone who cares about using digital approaches in the public sector to deliver better outcomes. I’m your host, Olivia Neal. I hope you’ve been enjoying our recent dives into the world of critical infrastructure, with our guest host Jeremy Goldberg. More from him coming up. But this week we’re back looking at broader issues for digital transformation the public sector.

Today we’re going to be looking at the use of cloud for different levels of data, and hearing from Rear Admiral Antonio Gameiro Marques, the Director General of the Portuguese National Security Authority about the experiences of his team, as they’ve tested different approaches to using the cloud for restricted data.

In discussion on use of data, the language and definitions used often vary by country and by agency. For clarity, in this episode where the Rear Admiral discusses ‘classified data’, what he is referring to is data that is commonly known as ‘restricted data’ in other parts of the world. We are not referring to mission classifications such as secret and top secret in this episode.

So with that clarity, and without further ado, Rear Admiral Antonio Marques, welcome to the show.

**ANTÓNIO GAMEIRO MARQUES:** Yeah, thank you very much for inviting me here, it’s – it’s quite an honor to be invited by Microsoft and having the opportunity of sharing some of our ideas which such a large and –diverse audience, for all of those that are willing to spend and and invest some time to – to listen to us.

**OLIVIA NEAL:** Well, I know that there’s been so much progress in Portugal that many people in other countries are really interested in learning more about. So this is a – a fantastic opportunity for us to share those lessons and for people to understand more about the approach that Portugal has been taking. And so to start off with, maybe just to give us a little bit more context around the area you’re – you’re working in

**ANTÓNIO GAMEIRO MARQUES:** I’m the – the Director General of an entity in the port—the Portuguese administration that takes care of the life cycle of classified information, and also, we have, within our structure, the National Cybersecurity Center.

I report to – to the Prime Minister through the Secretary of State of the Digital and Public Sector Modernization, which is a new role that has been created where everything related with digital is integrated. So there are several – let’s put it this way, independent entities, but they work together, namely for accessing cloud. So we are about 110 in total. well, that’s us in a very, very little nutshell.

**OLIVIA NEAL:** Could you tell us a little bit about how you’ve seen the evolution of approaches to technology, to architecture, to cybersecurity, within Europe, in that context, and then a little bit about how Portugal’s approach fits into that? Because I know you’re really leading the way in some of these areas.

**ANTÓNIO GAMEIRO MARQUES:** Well, basically, I personally sit in a – in a relatively wide-angle view, because not only my organization sits in the boards in the committees that deal with cybersecurity and – and information security in general, in the EU and also in NATO. So we can complement the views of both entities by grabbing what is more valuable from each one and then combining them together. And I have a very clear example on that.

On the classified information side, we have to certify IT systems to process, store, transmit, receive classified information. And this is done today according to NATO rules, NATO controls. On the other side, the EU is developing schemes to certify under the cybersecurity scope, not only services, but also items. the common criteria has been done already. Now they are working in cloud. They will work on 5G, on IoT, and so forth, and – and the goal is for citizens of the European Union to be able to know what is the level of trust that the system or the service connectable to the internet can give to them by – by three levels

So what have we done? We started the journey with Microsoft, by the way, in June of 2019 by experimenting the certification of some cloud services of Azure, not only for us to learn how to do it, based on the NATO controls, but also to – and we did it with Microsoft and we did it through the lab connected to one of the universities of – of this country, for the three entities to learn how to do it, you see?

It was a long journey, a journey that lasted almost a year because we were literally exploring things, like we were in a jungle and exploring things, you see?

And then sometimes we had to – to come back to the drawing board to see, well, this is not the correct way of doing this. , but we learned a lot. And by the end of the – the period, we had some services, quite a great number of Azure services, accredited to store classified information up to national restricted.

We were not very ambitious as far as the level is concerned. We were more ambitious in the process and in the controls we would use to do it. And then we stopped and – and the three entities evolved. So us, Microsoft and – and the lab connected to the Porto University that worked with us, we got together. We – we identified what went well, what went wrong, at – for us to in the following iteration to be more prepared.

And now we are already in the second iteration, and things are – are going much smoother, and yet the same time, you see – at the same time, how is this connected to the EU cybersecurity scheme certification? Well, the way we are thinking about it is – is the following. When the EU defines this – the cybersecurity certification schemes, for instance, for cloud, we will do it, up to the highest level. And then for classified information, we will only require the over and above, you see?

So imagine a pyramid where the top is the classified information, so we’ll do the – the – the top notch for cybersecurity certification and the delta for classified information, but the – the good thing is that, instead of waiting for that to happen from the EU, we are already doing it. We are already learning with that process. And this process has been so fruitful that, by the end of 2021, based on the national cybersecurity framework that has been developed, we work with the – with the authority in Portugal that establishes certification schemes, and we developed a formal certification scheme for – schemes for small and medium enterprises, our cybersecurity, and they are – there’s a label.

They are already doing it and there’s already a line for enterprises to enter that scheme, so – because they know that, by adding the stamp, the public and the market perceive them as more reliable than others that don’t have that label, you see?

**OLIVIA NEAL:**  So the EU are in the process of developing a series of schemes and cybersecurity being one of those, and in advance of that, within Portugal, you’re working with the lab at the university, with Microsoft to go further ahead on this certification process and get that in place now, so that you can start adjusting and start having the right technology that will give you the best benefits for the right levels of data.

**ANTÓNIO GAMEIRO MARQUES:** So basically, instead of waiting, we went and – and got some – some exercises done before – before the exam comes, you see what I mean? So I’m doing some – some kind of – you know, comparison with the – another – another type of - of activity.

**OLIVIA NEAL:** And so – so when you started this process of bringing the three entities together, the lab, the technology provider and yourselves, the – with the aim being that you would have a – a good solid understanding shown in the – in the form of certifications which IT systems could be used to process which types of data.

And you talked about having gone through the first iteration of that process, and – and that thinking about what’s the right part of partner to involve in that, what’s the right type of lab? I wonder if there’s any other lessons that you could share from having gone through that process, that – if somebody in a different country is listening to this and thinking, I’d like to replicate that approach in my country, are there any lessons that you have on where is the right place to get started, or what the right questions to ask are?

**ANTÓNIO GAMEIRO MARQUES:**  what we did, and I’ve – when – a member of my team, he did a lot of research, prior to – to starting the journey. In order us to assess or to – to compile all the documentation and all the controls, we should have in place on top of the table to start that – that process of certification. And we went to the EU, we went to NIST we went to NATO, and after a month or a month-and-a-half or so, we came up with a set of controls, that afterwards, through the process, with Microsoft, with the lab, we were changed or moved or reiterated.

And now we are in the – in the stage where we are already able to write documentation about it, so and doctrine says that when you reach the stage, when you are able to explicit what you have done in a logical and structured and understandable way, it means that you’ve done - you’ve done already a good and solid path, which - which means that now we - we are in the situation where we could show to others what what we have written, what we have put in – in the document for others to criticize in order for the document to become a better document in iteration, okay? And that is what we’re doing.

The plan is to have a document with inputs from the cybersecurity community. So remember, I told you the organization has two parts? So one part of the organization, the classified information part, produced the document based on the knowledge they have developed through the process of the certification they have done so far. And now I’ve given that document to the cybersecurity community and told them, "Hey, give me your contributions, your inputs." And – and then our intention is to open that document through other communities, okay?

**OLIVIA NEAL:** so that would be something that others would be able to access and – and challenge, but also use and be inspired by it.

**ANTÓNIO GAMEIRO MARQUES:** I think that part could be done a different way. Yeah, great. So now the document is written in – in – in Portuguese, but it’s going to be translated for it to be more widely available, and for everybody to – that is willing to do something positive, with respect to it, can access it, yeah?

**OLIVIA NEAL:** And I wanted just to kind of, on that type of topic, whether you could share a few of your thoughts around the role of using cloud and cloud-based tools, and the relation of that to cybersecurity and – and the pros and cons of use of cloud in your space.

**ANTÓNIO GAMEIRO MARQUES: the** cloud, I’ve made a part of a team in the government where we have developed frameworks and for cloud – cloud approach to – to… for government use, government – let’s say the – the – all the entities that are part of the Portuguese state.

And – and my opinion is that anything that doesn’t lead - doesn’t deal with sensitive information can, in general, in general terms, can go to the cloud. However, what is for me the most tricky thing about cloud, where is not only the data, but the metadata stored

And this is – this is the key aspect, as far as I’m concerned, because– data in a context is information, and information produces knowledge, and knowledge produces wisdom. And if that chain of value, including the metadata, is in other geographies, but the European geography, I have some – some – some worries about that.

we have to be intellectually honest with ourselves and do this thinking, do this reflection, you know, these deep thoughts, instead of being dogmatic and saying, no, I wouldn’t want anything of my data in – in the cloud where I cannot see where it is

**OLIVIA NEAL:** And presumably in a thinking those things through, there’s – there’s always a balance when you are looking at the level of the sensitivity of the data –

**ANTÓNIO GAMEIRO MARQUES:** Yeah, sure.

**OLIVIA NEAL: the** considerations, and then also the advantages, as well, and weighing those things up.

**ANTÓNIO GAMEIRO MARQUES:** Yeah. And within that group that we have still working, we developed a framework whereby questions and answers, one can have a leader, a decision maker can have a very pragmatic idea of if he or she should use cloud and what type of cloud for the specific types of data that – that they have.

I wish I could, you know, I could only focus on the systems and data that are unique to this organization.

It should only be my organization as things that all organizations have and things that only us, only this organization has. So, these are the ones I have to look into. the others, well, let’s put it in the cloud. It’s less money for me for maintenance. I don’t have to – to change the hardware every five years or seven years. I just use. And I can concentrate my human resources on the things that make us unique and are the reason for us to exist in the government of Portugal. You see what I mean?

**OLIVIA NEAL:** And – and you’ve done a number of different posts within the Portuguese Navy and the Portuguese government. When you come to the end of this post, hopefully, you know, not for some years, but when you look back on this post, what do you hope you will have achieved within it?

**ANTÓNIO GAMEIRO MARQUES:**

I’ve been CIO of the Navy. I’ve been assistant secretary – secretary general of MoD Portugal. And now, I’m in my sixth year, my sixth here. So, I’m – I’m actually in last part of the second term

And the key part here is to trust – to – to trust your people, empower your people by putting them to places where they can learn, they can be good leaders, good managers, good technicians and – and monitor what they do, monitor in the sense of not with censorship in mind, but with the empowerment, with trust inside.

Of course, as in all areas, there are human beings that react differently from these stimuli, but what I can tell you is that the majority is quite positive with this attitude, you see. Let them do it. Give them direction. let them know that you are here, if they need guidance. be close to them. Don’t spend your time just in this building, in this room. Go, talk with them. and that’s what I’ve been doing since, what, since 2008.

**OLIVIA NEAL:** Well, I have one final question, which is you talked about your – the community of people working on cybersecurity and the value that you get from that, and how you’ll be opening the work that you’ve done in your documentation to look for challenge and help to improve. Is there anyone out there that you look to for inspiration? Are there any other governments who you think do this really well and you look to them to see what they’re doing?

**ANTÓNIO GAMEIRO MARQUES:** Yes. Yeah, yeah. What – what I’m going to going to tell you, it – it’s a reflection of my path, my professional path. And I’m a naval officer. I studied in the U.S. in the ‘80s, but then I worked in the ‘90s a lot with the Royal Navy. And – and after, I was in NATO. And a lot of the doctrine NATO has comes from the British standards. I think the – the – the doctrine that generally is produced in UK, including cybersecurity, is very good for inspiration, at least for my inspiration.

The Dutch, I’ve lived in the Netherlands for one year and a half and I also like the way they approach things.

but my inspiration comes from the fact that I like to read a lot and to listen to a lot. Nature has given us two ears and just one month. So, we should hear more than we talk. And I learned a lot just by listening to others. And it’s also an attitude because I’m eager to – to learn new things.

**OLIVIA NEAL:** That’s great. Thank you. And that’s been a fantastic set of – set of insights. Is there anything which I haven’t asked you which you would want to share or anything that you would want to get across?

**ANTÓNIO GAMEIRO MARQUES:** Yes. I – I would, for all of our listeners, I think invest in people, invest in the knowledge of – of people, of your technicians, of your workers, of your personnel, because that’s the best investment you can possibly do. It will probably not get a return in the near, near future, but will – but it will get the return for the society, for them and for the organizations they – they’re working.

And that’s reason why we are starting quite an ambitious advanced cybersecurity education program here in this country that will be delivered through the Polytechnic Institutes and universities of this country, based on the cybersecurity framework that we have developed. And we, above all, we will enable society to be more capable, as far as cybersecurity is concerned, and to sustain the everyday attacks that are suffered throughout the world.

Well, thank you so much for your time.. Thank you. Thank you for being here. (Laughter.)

**ANTÓNIO GAMEIRO MARQUES:** Thank you very much, Olivia.

**OLIVIA NEAL**: Thank you to our guest, Rear Admiral Antonio Gameiro Marques, and thank you to you for joining me today on Public Sector Future. Our goal is for you to learn something new and to be inspired to think differently about your journey.

If you enjoy today’s episode and want to help other people find it, please share, rate and review the show. It really does help people discover new shows like this one. Check out our show page for links to all of what we discussed today. And visit us at wwps.microsoft.com. Please do reach out send us your questions and your feedback. You can find me on Twitter @LivNeal or on LinkedIn, or you can email us at ask-ps@microsoft.com. Thank you and see you next time.

END