Transcript: HCLTech x Microsoft Sovereign Cloud Podcast

Moderator: Dr Andy Packham

0:05
Hi, welcome.
I'm Andy Packham and this is another in the Elevate podcast series where we focus on the Microsoft ecosystem and how HCLTech and Microsoft have been working together to solve real problems for our customers over the last few years.
Sovereignty, sovereign cloud, digital sovereignty has been really emerging as one of the central themes that organizations are facing jointly, of course, with artificial intelligence.
And it's the it's been at the forefront of many conversations.
The rise of AI has only intensified that debate as businesses are grappling with questions that we've never really focused on before about controls, operational transparency, responsibility and regulatory security.
But like, unlike other areas for sovereignty, there is no universal standard.
It's not like there's a template that we can apply and it impacts globally and it impacts organizations in many, many different ways.
There's no fixed requirement, it's not something you can simply purchase and switch on.
So each company needs to kind of figure out it's only it's own path through there.

And that's what I wanted to focus on in on this discussion today is how we go about navigating those complex issues.
So I'm really excited.

I'm joined by two key experts, firstly, Thomas Maurer from Microsoft, with incredible deep expertise in Azure as your local and how that platform capability supports, compliance and control and from HCLTech Rajan Pillay, who works with global organizations and operates at that level of complexity, multi-region environments and regulatory and business concerns.
So both of you really appreciate you taking time and thank you for joining.

To kick off, I'd kind of like to start by getting a, you know, each of you tell, tell me a little bit about your role, the conversations you're happening, you're having about sovereignty with customers at the moment.
So Thomas, do you want to do you want to kick off and tell us a little bit about where things are you and your perspective?

Speaker: Thomas Maurer

2:20
Yeah, absolutely.
So thank you andy, first of all, for having me today on this podcast.
I'm really glad to be here.

Yeah.
So I'm working as a TVB, which stands for Global Black Belt in Microsoft and focusing especially on sovereign cloud.
And before that I was actually working in the engineering team for Azure Local and Azure Arc.

And there is some advocacy work before that account like Azure operations in general.
So yeah, I have a lot of these discussions today with different customers from all different industries to be honest.
It's not just limited to like public sectors like many of people may think.
It's really like across all these different industries.
And what's for me is, starting thing is really that, hey, there's not and you mentioned that early on in the conversation, is that not one thing which, OK, sovereignty addresses this one thing, right?
It's really about finding the different use cases in that journey.

What problems do the customers try to address?

What are their challenges when it comes to sovereignty?

And so that conversation is really what happens most of the time.

Moderator: Dr Andy Packham
3:32
Awesome, great.
Rajan, do you, are you seeing the same thing in the conversations you're having with customers?

Speaker: Rajan Pillay

3:38
Yes.
So again we see a lot of demand coming up from the Europe and enquiries right now understanding how we can help.
Again, I would say still a maturing area, not something everyone has achieved or not a solution which has matured over a year.
But customers are understanding what can they do, how do we help them and what is available with the players like Microsoft and everyone in the market and we are glad to help and have that conversation with the customer.
So my role, I am part of HCLTech Digital Foundation Services.
I head the technology for the hybrid cloud unit and as well as head the solvent cloud business for HCLTech.

Moderator: Dr Andy Packham
Awesome, Rajan, thanks.
So, so sovereignty is contextual.
Yeah, I think we've all we've all said it, it's there is no, there is no standard.
But what are the non negotiables whatever what you know, what do you see that every company must demonstrate that sovereignty sort of in a way folds into and how do you go about doing that?
Ranjan, if you want to you want to pick that up first.

Speaker: Rajan Pillay
4:54
Yeah, So the non negotiables are very clear.
You must be able to prove where the data resides, who can access it, who controls the keys, how the compliance is continuously monitored and can be audited.

Trust or today has moved from say you cannot just say I have evidence for in 70, but it has to be more how we can prove that right where the proof comes, the proof can be through implementation of policy as a code, compliance assessments and records which are available for auditable as well as auditable logs.
The 70 control model is say built around say data residency encryption.

Confidential computing is also gaining a lot of traction to say how you take care of data and use it as well.
And then there are capabilities like say data garden locally supervised access or tamper evident proof logging.
The conversation has moved from say intent to providing the proof and it's no longer enough to say we are compliant by design.
But you need to have the policy, the exception handling capabilities and also show the live evidence and audit trails for your sovereignties.

Moderator: Dr Andy Packham
Yeah, I read, I, I think that that word trust is, is is key in this, isn't it?
It's so important then and it and it and it works.
But it works like exactly like you said in two ways.
Everybody wanted to trust, but we still need to check.

So yeah, Thomas is, is that the same pattern?
Anything to add on that?

Speaker: Thomas Maurer
6:43
Yeah, no, I, I think this is this is very much true.
And I like the trust here.
I think that is very important, right?
You can have all the regular regulatory requirements and all that, but if you don't trust someone, I think that's not not going to work out very well.
So I think that is something we really understood and that's what we also try with Azure, right.
And when you look at our sovereign cloud story, we offer these parts in different ways.
So we have our sovereign public cloud, right, where again, we talk about these, these and then we'll talk about this in just a bit, a little bit more, but where we actually use our general public cloud, not specifically built public clouds, but really like the general Azure public cloud and making these sovereign capabilities built in to say, hey, everyone can use them, right?
Like it should not be like, hey, OK, you're that important.
You go, you go to a sovereign cloud, but it's like, it's like sovereignty for everyone.
And then we also, however, know that there are different requirements where you need to run on Prem and disconnected environments, right, where you have other locations and so on.
And that is where our sovereign private cloud story comes in.
And then the third pillar we like to talk when we talk about sovereignty is our partner.
That pillar, right, where we work with our close partners, which are very important to drive our sovereign cloud portfolio and help customers.
We understand because we as Microsoft, we cannot understand everywhere, every single scenarios, customers, partners have much more knowledge in that space and can help really help customers to address this.
Now to go back to your question, Yeah, so I think there's another part which came up, right.
We was allowed transparency.
And I think that is where Azure really can provide like we have this transparent controls built in which

first of all, like we afford a general cloud.
We have our trust center where you can read about this.
But then especially for your environment where it's about like proving that you're actually configured the right way.
That is where for example, we have Azure policy and policy enforcement where you can figure out, hey, this is actually configured the right way.
And the great thing about this like how the way we think about Azure and I just mentioned these three big pillars, right, with the power sovereign public cloud and the sovereign private cloud is that we, we years ago already spend like spend time building this control plane, which goes across the different environments right from public cloud to on-prem to edge to even other cloud providers.
And then really helps you to identify and use the same toolings and then identify, hey, am I compliant with these requirements, right, to help this in this case.

Moderator: Dr Andy Packham
9:24
So Thomas, just one point in that I think it's important you talked about Azure as your sovereign.
So can you, can you do sovereignty with cloud?

Speaker: Thomas Maurer
I like this, this, this the phrase you phrased the second part of the question much better because sovereignty again, as we discussed, right, can mean different things for different people and different, you have different use cases.
In some cases, you need data sovereignty, you need operational sovereignty.
So when we speak about the public cloud, what we offer is what I call, there's basically two things.
The first thing I call is like the things the customer gets for free by using Azure.
There was mention of Data Guardian, the data boundary in Europe, right, which things are just built in into our Azure platform, so that once you start using Azure in this regions, you already can benefit from this, right, without doing anything.
And then the other part we're looking at is, OK, we need to help customers to protect their data, for example.
And so that is where different encryption paths come in, where confidential compute comes in and so on.
But what we also understand is, OK, this is maybe not like every for every workload, right?
There's like different types of workloads. So you might have, as I mentioned, scenarios on Prem.

So you have, for example, Azure local, which can help you deliver that infrastructure and AI capabilities. And with M365 local, even productivity workloads running on premises.
So you can design and address these different sovereignty challenges definitely with Azure, right.

Moderator: Dr Andy Packham
11:05
So Rajan in those conversations that you've been having, how do you say that you know, that maybe it's easier sometimes just if I've got a, if I've got a regulatory like workload, I'm just going to keep it on Prem.
How do you respond to that?
How do you kind of say, you know, we can, we can have a different, a broader conversation about that?

Speaker: Rajan Pillay
11:29
So it's not about everything being on Prem or which location or does the location itself assure sovereignty, right.

So you can keep something in region on-prem, maybe that addresses one requirement, but it doesn't automatically give you better governance, better auditability, better control or better resilience for matter Microsoft Framework or what Thomas just explained here.
There are various options, be it local, private environments which can give strongest control over infrastructure, data, operations.
But it also comes with trade-offs like is it scalable?
Can you do the same level of innovation and does it allow the same speed or agility?
And is it cost effective, right.
So maybe on prems and some of the controlled environments may be more expensive.
That is why it's not that it's not a all cloud versus all on Prem kind of debate.
It should be based on what workload placement makes the right decision.
Some cases private, maybe right, some cases public can do.
And there are many regulator workloads which customers even today run on public cloud and same would be we feel in the sovereign.
Also many regulator workloads can be run on a sovereign public cloud model with the right guardrails and where customer has full controls and has the operational autonomy or even fully.
There could be requirements of fully disconnected operations where solutions like on Prem solutions like Azure local or solvent private cloud and various solutions which HCLTech also provide scan come into picture.
The important point is to have a consistent operating model across the hybrid private disconnected environments rather than creating islands of technology.
So that's what happens, yeah.

Speaker: Thomas Maurer
13:39
And, I might I add to that because I like this, this very much how you answered this.
And I, I think it just give you, I want to also give you some like examples for like where obviously cloud provides a lot of things like you mentioned innovation, right?
But then also when it comes to security, right, there's another part which people sometimes don't think about is like, OK, hey, what if I run now completely disconnected?
How do I get all this security I get from the cloud, right?
And there are certain tools which can extend, but there's no way you can, for example, get all that in a disconnected environment.
So you need to think about that clearly.
The other part, which I'm also looking at is we talk always about this.
And I, I do that because I talk a lot about actual local.
We talk about like resiliency, like to what's, what if there is a cloud outage, right?
Let's say, OK, cloud is not available, OK, how can I continue running on prep?
Now what we also see and when we especially when we have these more serious discussions and also from the the last couple of events we have seen, there's also scenarios where the cloud is actually the one place to go to because it makes it easier to move your data from one region to another, right?
Think about disasters, geopolitical factors, right, where we have seen customers actually moving or be preparing to move data out of that specific region and move it to another cloud region which is further away.
I had some interesting conversations about like, for example, designing for earthquakes, right?
And things like that.
That also is in some things you need to discuss is like, OK, what happens if I'm just designing?
I want to keep all my data locally. I just want to keep it up myself.
I want to even if I used the same as region, there could be a disaster or something where I'm actually happy to have everything further away.

So there's these kind of things and I think you mentioned that really nicely that you need to design for these different purposes and use cases.

Moderator: Dr Andy Packham
15:38
And so Rajan, I want to stay with you on also something else you said.
And I think it's important if you look at, if you look at most of our customers, large organisations, it's not that they just have an operation in one country or even in one zone.
They may, you know, they, they may be in the Americas, they will be across Europe, they will be in Asia.
So how do you think about that when it's not just one sovereign kind of requirement?
There's a risk of huge levels of complexity and fragmentation if we kind of create 20 or 30 sovereign solutions.
I'd like to get your views and and kind of, you know, how do we do this but also control costs and keep agility there.

Speaker: Rajan Pillay
16:22
Yeah
So the answer would be to try to standardize globally and try to apply policies locally, depending on the industry, depending on the countries you operate in, right?
Not by rebuilding the stack individually, country by country.
Fragmentation usually happens when every geography tries to create its own tooling, its own landing zone, its own operating model and its own reporting.
That is very expensive and very hard to govern.
A better model would be a common cloud foundation, one security operations model and then local controlled layer which is required.
Examples say Microsoft Sovereign Landing zone is built around the layered policies.
Regulatory environment management is meant to unify how Sovereign workloads are configured, deployed and monitored.
Then that matters because say there are Euro Data Act is also pushing the industry towards in probability easier switching of moving of the data.

The long term answer could be cannot be duplicated silos.
From HCLTech perspective, the real differentiator is also our operating model, common engineering, common governance, common phenops, but with local controls for residency, encryption, privilege access and sector specific rules.
So it means the standardization as much as possible and apply regulations, policies which are very specific to industries and that country.

Moderator: Dr Andy Packham
18:06
Thomas, how does that sound?
Does that you know, in terms of what you're saying from the platform perspective, is that is that achievable from Azure?

Speaker: Thomas Maurer
18:16
No, of course, yeah.
So I think this is really where the investments from the last years paid really off, right?
I think it was in 2019 if I remember correctly when we launched Azure Arc.
Actually Azure Arc and Azure Arc really provide is one part which really provides that common control plane across these different environments and extends the Azure control plane basically to these different environments.
Doesn't matter if it's on Prem edge or even multi cloud scenarios.

Now multi cloud is another topic where obviously there's a lot of discussions which need to go in there, a lot of skills which are needed.
But again, if you look at this like I have seen customers having tooling like four or five different toolings to do the same thing depending on where their workload is running, right.
So let's say just simple 1 update management, for example, they had an update management solution for the workloads in Azure, one for on Prem, another one for like their edge locations, one at another cloud provider.
So that is something we are addressing with Azure and especially with Azure Arc extending that control plane.
Now this is like I was speaking now about operations, but obviously this is also true then when it comes to compliance, right.
Imagine, I can only imagine how hard it is to keep compliance under control if you have these different environments, right?
It's already difficult to be honest for one environment in some cases.
But if you have all these and then you have different tooling in place, that is going to make it very, very hard.
So that is where again, the control plane can really help.
And the way we look at Microsoft Azure, Azure Local and together with Azure Arc and all these things, this is really what we can bring together.
And that allows you then to enforce these policies.
Like first of all, audit these environments, but then also enforce these policies together.
For example, also as you mentioned with our Azure landing zones or Sovereign Cloud landing zones, I think that is really a unique value the Microsoft Cloud can offer in this case.

Moderator: Dr Andy Packham
20:22
So to wrap up just a few words, you know, Rajan, if we start with you again, what advice would you give to a customer, especially around how do you balance sovereignty, compliance, the need for agility, the need for innovation?
There is so much to balance there.
How do you go on and you know, how would you advise a customer and what would you advise them to sort of think about as priorities?

Speaker: Rajan Pillay
20:56
Yeah, So I'll suggest, say 5 practical steps.
First, classify workloads based on regulation, business criticality and geopolitical exposure.

Second would be define the evidence model clearly.
What exactly do you need to prove to auditors, regulators, the leadership and say the board?

3rd would be to make a guarded public cloud your default or whichever private or hybrid model suits you and reserve solvent private cloud or discount environments for workloads that clearly require that kind of control. So to basically put the right workload placement placement strategy, right, So you can definitely look at public cloud or Europe specific regional clouds which are available.

4th would be start with a policy in audit mode, understand the operational impact and then move to enforcement of large scale right.
Even too much security policies may slow down the innovation, the pace, the latency, all other issues.

So you have to have the right guardrails, the right auditing which is needed, not over engineer it.

And the 5th is designed for resilience, portability and cost control from day one.

Any outages, disaster, wow, it could be anything, right?
Power outage which can have impact.
How do you ensure you are resilient and running but still doesn't have a exposure from the sovereignty perspective.
And the next phase would be the phase of regulation, which is much more focused on the operational and interoperability and it is also about data residency.
So done well solvent P should make innovation safer and faster.
But if it over engineer too much controls, then it may create very expensive form of fragmentation.
Finally, I'll say sovereignty is not about putting everything behind the wall.
It's about applying the right level of controls, proofs and resilience to the workloads that matter most.

Moderator: Dr Andy Packham
23:07
Yeah, Thanks, Thomas.
The same would you say the same things?

Speaker: Thomas Maurer
23:15
This was a very, very nice summary of the way to think about this.
Usually what I would say is be really aware of one of the first step, what you're trying to achieve, right?
I know I'm going to repeat myself here, but knowing about the different use cases you want to address, this is a very important part because you can very quickly go down a rabbit hole where you will always find something wrong, right?
And so you need to figure out, OK, what do we want to address?
And then the other thing which I liked also before is like avoiding try to because it's already complex enough, try to avoid complexity, try to build a solutions which help you to basically use one single tooling build like the set, use the same processors independent more or less from the different locations you are using, right.
And so I think that is something where if you choose a good platform to operate on, I think that is that is very important.
And then also make sure like as a customer, for example, like make sure, make sure you choose the right partner in this case, right?
We have very good partners who can help you have experience as HCLTech does to like deliver these sovereign solutions, help with resiliency, help with all these new workloads and build these designs you mentioned landing zones and so on.
So I think that is that is also something I highly recommend getting started with this with no prior experience in this can be can be very hard.
And then last but not least, I mean, we're not talking about these, these scenarios, but also think about what might be coming, right?
Think about like how can you address future workloads you might not have now, but maybe you will have such as AI workloads, you might will have requirements from the business side, how to address these.
And then also, I think what is a very good point also these things are there to change, right?
Requirements change what I designed today is maybe not true 2 years from now, right?
Maybe we have different scenarios.
So be prepared to change in these, in these, in these different scenarios and models and your architecture, right, that you can actually go and and address these.

And again, this helps if you avoid complexity or try to avoid complexity, that's will help you a lot over the long term.

Moderator: Dr Andy Packham
25:34
Thomas, thank you for that and Ranjan also for your comments.
So I think these are all really, really important that, you know, if we kind of go back when we used to think about resilience, we kind of thought about resilience as a network failure or the database failure or power failure now.
And what I'm hearing is that and what drives a lot of this conversation is we need to think about resiliency on a far more broader scale, you know, whether or not that's the, you know, the ability to be resilient in, you know, in, in a geopolitical upheaval or, or changing compliance or business priorities.
So rather than just now thinking about kind of resilience from what was like a technology with, we're thinking about creating through technology a layer of business resilience.
And I think that's really important.
And the fact that, you know, that means it's not done if you just kind of like, you know, you put two data centres in 1/2 are both operational.
Now we're talking about resiliency as in continuously evolving what we need to be resilient about.
So I, think that guidance is really, really important and very, very helpful.

So yeah, I'd like to thank you both.
This has been an absolutely fantastic conversation.
And, you know, I can certainly see this whole, this whole subject of sovereignty and resilience and agility and compliance.
They are they're very intertwined.
And all those, these new workloads come on board with AI and everything.
I think this is certainly going to continue.
And you know, the final point and Thomas, you made this really well.
Yeah, this is all about, this is all about partnership, you know, with Microsoft, we're with ourselves in partnership with customers and the regulators and and many other external bodies.

This is something that we are going to have to solve together.
It's not just a it's not just install a pattern and we're done.

So Rajan, Thomas, thank you very much for the conversation.

I've really enjoyed it, learnt a lot from it.

And I hope everybody who is listening this will also learn a lot.

Thank you very much.
Thank you.

Speaker: Rajan Pillay
27:45
Yeah.
Thanks Andy.
Thanks, Thomas.

Speaker: Thomas Maurer
27:46
It was great to be here.
Yeah, Thank you so much for having me.