PRIVACY SIGMA RIDERS EPISODE 4: GDPR... Better Than a Poke in the Eye with a Sharp Stick

Michelle Dennedy: The EU general data protection regulation enforcement is just around the corner. Companies large and small need to rethink their own privacy frameworks, and not just from a compliance standpoint, but from the ability to compete in a changing global market. Cybersecurity, data protection, privacy. You like to stay ahead of the curve, and listen to experts who are leading the way in deriving greater value from data with a more organized approach to data privacy. You're like us, just a few deviations past the norm. You are a privacy sigma rider.

A hot topic in data privacy is the impending EU general data protection regulation, affectionately known as GDPR, which will be enforced in Europe beginning next May, 2018. This law offers a new framework for companies to manage EU personal data. The GDPR also brings a new level of accountability, and a new cost of accountability, that all organizations, even those that don't do business in Europe, must pay attention to. Today, I want to talk about the GDPR and other global data privacy initiatives, and how we prepare for our changing global landscape. With me is Lorena Marciano.

Lorena Marciano: Hello, Michelle.

Michelle Dennedy: Hello, Miss Lorena. Lorena is Cisco's data protection and privacy officer for EMEAR and she works with customers and partners in that region, helping them understand the GDPR and the impact on their business. She's been with Cisco more than three years, having previously served as Senior Corporate Counsel. With us also is Harvey Jang.

Harvey Jang: Hello. I'm glad to be here.

Michelle Dennedy: Hi, Harvey. It's good to have you. Harvey is Cisco's Legal Director for Global Privacy and Data Protection, and he's also our data privacy officer for the Asia Pacific region. So, welcome Harvey and Lorena. Let's get started on the party towards GDPR. Maybe just to level set everyone on what the GDPR is, Lorena, can you provide us a quick overview of kind of a long law?

Lorena Marciano: The GDPR is a new law, that's true, but in terms of content it's not really new. It's something that we've had in Europe for the past decades. What is really new about GDPR is that it's consolidating to any eight privacy laws that we had before. It's a big achievement for us because if you think about how the use of data has become so important in a data-centric economy, be able to apply only one law just to any jurisdiction, it's a big, it's enormous achievement because it gives consistent, and to some extent, it gives stabilities to the business that operates in many countries.

Michelle Dennedy: So, there's some stability, but you mentioned some significant fines and penalties for noncompliance. Can you elaborate a bit more? That one piques everybody's interest, I think.

Lorena Marciano: Yeah, it is. We have a very high level of fines. It's 20 million or 4% of global turnover.

Michelle Dennedy: That's a lot of turnovers.

Lorena Marciano: It is, especially think about the small and medium size. Maybe 20 million doesn't speak too much in bigger enterprises, but if you think of the small one, it's a big hit. Even if you think of the bigger one, 4% of global turnover sometimes it's the entire revenue of one theater or one region.

Michelle Dennedy: That's pretty incredible stuff. It's one of the most extensive data protection overhauls, as you say, Lorena, and Harvey's experiences along the way, too, both very seasoned people. This isn't necessarily new content, but, boy, oh, boy, with the penalties raised to these levels, as well as the consolidation and instant applicability once the law is being enforced, we've really moved beyond an area that this is simply a checkbox compliance-type of activity. It sounds like doing right by your customer really requires you treating the data as if it was your own. How is that GDPR helping to codify this? How is it steering practices, and what's the view on the ground? I mean your accent, it sounds like you're from like the Bronx in New York. Is that right, Lorena?

Lorena Marciano: Not really. Quite. No, it's an Italian accent, indeed, of someone living abroad for a very long time. But that's right. It's changing the way we should think about the use of data, and it's bringing the decision-making and the accountability back to where it's supposed to be, so on the company that will use the data for their solution for creating better services, and it helps in many way. We're talking about this over ... you know last night.

Michelle Dennedy: Harvey and ...

Lorena Marciano: ... during the meeting that we had and we're talking about how important the accountability and how it's important also to achieve certain things. Because if you think about, I am a company, I'm in charge, I need to think about privacy and privacy controls and the solutions.

Harvey Jang: Yeah, and I think with GDPR it introduces a level of accountability and a risk-based framework that we didn't see before in Europe. I mean in Europe historically focused only on privacy as a fundamental human right, and almost, in some cases, over-rotated on that right, and what we're seeing in GDPR is a balancing that's being introduced. Like some recitals ...

Michelle Dennedy: When you're saying over-rotating just to kind of jump in there, do you mean it over-rotated by giving too many rights, or because it was an absolute right without balancing against other ...

Harvey Jang: Right. That they were treating privacy almost as an absolute right, and not balancing against the rights of others, the interests of business and economy overall.

Michelle Dennedy: And even national security issues, right?

Harvey Jang: And national security, and so, you see even in the recitals of GDPR, it does made clear that privacy is a fundamental right, but not an absolute one.

Michelle Dennedy: For the non-lawyers out there in listener hood, recitals is just like a string band? I don't know how those work.

Harvey Jang: The recitals go in front of the articles, and the recitals give the history and the background and the purpose of the legislation. The actual articles themselves are the law, but the recitals tell where the legislators were coming from, what they were thinking, and the impetus behind the law.

Lorena Marciano: And also the recitals are often used, and it's a good point that you raised why it's recitals important. It's something used by all Europeans to really interpret some clues in some articles that are a bit not clear and so if we can give one tip to the companies that are preparing, it's really to take into account on all of the articles, but to read all the way to the beginning. I know it's a very long reading, but do it. It's really important to understand the concepts.

Michelle Dennedy: I thought everybody was reading the GDPR and its recitals.

Harvey Jang: The fines are heavy, but I don't think it's something to be feared. If you actually take the time to read the GDPR, as all of us have multiple times ...

Michelle Dennedy: Doesn't everyone?

Harvey Jang: It breaks it down and it tells you how to mature your privacy program or even taking models and elements of any good compliance function that would be effective. What are the pieces you need? You need organizational leadership and I pilot. I think the French called it a pilot if you weren't going to call it a pilot

Michelle Dennedy: A pilot al avion

Harvey Jang: If you're not officially going to call it a data protection officer, but you need a leader. You need resources. You need executive buy-in and then pieces like: you have to understand your data and be transparent about it. What's interesting is this risk-based approach and so there's a different perspective on privacy and people weigh it a little bit differently and so you're going to have a variance in terms of what's expected. Across the board, people expect you to be transparent, fair, and accountable and the transparency is the critical piece that is the foundation behind much of what we're doing in privacy. Say what you do and do what you say and be accountable to it.

Michelle Dennedy: So does Europe have a lock on this? Harvey, you seem pretty conversant in the land of European data protection.

Harvey Jang: It's all convergent. Historically, we looked at privacy and globally, there were three paradigms. There were those that were pushing privacy as a fundamental right. There was those looking at it as global trade and on the other hand, also looking at it at risk of harm. Before, we were taking these three separate paradigms and it was an either/or, but now we're looking at it more as an and scenario, where, yes, it's a fundamental right and it's important to global trade and we have to be cognizant of the risk of harm for mishandling. We're seeing this convergence in our operability between the frameworks around the world. Actually, just going back to basics, going back to the eighties with OECD and those were the principles that were espoused thirty years ago are still true today and form the foundation of all the laws that have been coming on by more recently

Michelle Dennedy: I can't help but think there were some things that were great in the eighties. I'm wondering if you'd be willing to post a haircut photo?

Harvey Jang: The mullet was not.

Michelle Dennedy: It was a very interesting decade for fashion for us all.

Lorena, it's really interesting. We talk about these regional laws. It sounds like this is becoming a universal both a strategy as well as a risk. What are you hearing from customers? You know, you've got boots on the ground in the European Union and you're talking to customers every day. What are they saying to you?

Lorena Marciano: Well, there's certainly a current obsession with GDPR, so we talk ...

Michelle Dennedy: Which is kind of cool. I always thought we were high fashion.

Lorena Marciano: I know. It's very in fashion, and from an Italian, you know ...

Michelle Dennedy: She knows her fashion ...

Lorena Marciano: GDPR, it's written centered in all this discussion. If you look at it, really what it wanted to know is ... They always ask the same questions, right? They'd say at Cisco, "Well, I wanted to buy this solution for you," but in order to buy it, they need to have certain information. Why is that? It's because your solution will be used by my employees, by my end user and those are people that will ask questions. They know their rights. It's a fundamental right, privacy. They know their rights because we have decades of experience with privacy and we have made those people very savvy about it. They wanted certain answers and that's why I come to you and I wanted to ask you the questions that are always the same. What data your solution needs to use, for what reason do you need to use it, where do you store it, when can you really delete it, and who has access to it? Those have been the questions that have been going on forever and will stay.

Michelle Dennedy: That's interesting if you think about the ethics and the journalistic integrity. Who, what, why, where, and when, and can you prove it? Can you show me that you're doing what you're saying you're doing and you're walking in integrity so I can further that message to my end customer?

Lorena Marciano: It's like what Harvey already said. It's all about transparency, so if you want to earn my trust, you need to be transparent and you need to give me the minimum information in order for me to be transparent with these people, to the people that will use your solution.

Harvey Jang: We're seeing a push going from that trust or "Trust me. I'm Cisco. I've been here for decades."

Michelle Dennedy: I've got a good brand.

Harvey Jang: Right. It's moving to trust by verifying, how it should be, so we're seeing a drive towards external certifications and external validation of privacy and security laws.

Michelle Dennedy: That's a good point. So what are some other certifications that are out there? What are you seeing as our data protection officer in Asia Pacific?

Harvey Jang: Asia is one that is just now beginning to get a little more traction and we're trying to drive for a greater adoption and capacity for this framework, called the CBPR, the Cross-Border Privacy Rules

Michelle Dennedy: More acronyms? Harvey ...

Harvey Jang: Alphabet soup here.

It's the Cross-Border Privacy Rules system and it's based on APEC, Asia Pacific Economic Cooperation, and it's a 21 member economy, that countries that border the Pacific ocean that were able to participate in this group. They got together and came up with a privacy framework back in 2005 and they updated it in 2015. The nine principals in this framework match closely to OECD guidelines and are very much aligned to the European law and frameworks on privacy and principles of that. The certification, where you have a third-party accountability agent come in and review your program, review your policies and practices and confirm that they adhere to these nine principles. There's a lot of flexibility built into the APEC framework. You can imagine these 21 member economies, many of them not speaking the same language, some countries actively in conflict with each other and the challenges there.

Michelle Dennedy: Yeah. Some countries don't always play nice together.

Harvey Jang: Right.

Michelle Dennedy: And their data doesn't either.

Harvey Jang: Right. You can imagine 21 member economies and their heads of state to agree on privacy principles, they have to be pretty much universally understood or fundamental to the human right aspects of it.

Michelle Dennedy: That's right. So even the language, you know, 21 economies. We can't always agree on whether something should be designated a country or independent nation, but the economy of data is pervasive. We all want to communicate, oftentimes, across borders. It sounds like the future

trend is continually globalization with local characteristics. Does that sound fair?

Harvey Jang: That's exactly where the trend is moving. Even when new economies have joined this Cross-Border Privacy Rules system. They are also developing their own local trust mark to go along with it. Korea, as well as Singapore, who are recent participants in this, are working on their own localized trust mark in addition to this local ...

Michelle Dennedy: When you said it was trust mark, I thought it was like Walmart, trust mart. I would like a mart for trust, please?

Harvey Jang: So a trust mark would be a certification from an independent third party that comes in to verify that privacy and security promise, so then you can trust them because someone else has done the review and audited, assessed, and validated that they can live up to the promises that they made.

Michelle Dennedy: I like that. It's tricky as a privacy officer to look over this complexity that we're talking about, but at the same time, it's kind of comforting to say we're starting to have some sort of standards. We're having a little bit of harmonization. We're at least speaking in, sometimes broken language, but often a similar type of language that we kind of know and love and understand from back in the eighties and nineties when we first came up with fair principles and practices. I think it's really interesting and strategically, I'll ask both of you. Lorena, how can Cisco help with GDPR? What's a B-to-B gal like us doing in a place like GDPR? How can we help our customers?

Lorena Marciano: We can help our customers by providing to them this information that we have to do business efficiently, especially with our end customer. I think we can even share our experience, which is even more powerful if you think about. I know that sometimes putting together a privacy program is really sometimes related to the resources that you have. In essence, there are some things that you can do no matter what size you have to build a solid program.

Michelle Dennedy: I'm not even going to make that joke.

Harvey Jang: I think part of our job is to simplify the complexity. There's so many laws, hundreds of laws out there, but what's the common thread throughout and that's the transparency, fairness, and accountability. If we can make it simple for our customers to do business with us, and even provide a framework that a company that is leading in privacy is doing, then we can help set the standard, help set the example of how to be

transparent, to ensure that we're fair and how improve our accountability.

Michelle Dennedy: As sigma riders yourselves, I think it's really interesting, you know. We get a lot of flack and I think lawyers are the last bastion of politically correct humor and people will cast us as Doctor No. I'm hearing a ton of motivation out of you guys, so kind of final thoughts. What gives you hope in this space and what's next in these exciting edges in the part of your roles as you see them?

Lorena Marciano: I guess we are in a moment where all privacy professionals are in a moment where we have waited a very long time. We're in a moment where ...

Michelle Dennedy: You finally like us!

Lorena Marciano: Or at least you need to like us.

Michelle Dennedy: You need to like us, but it's like a kid sister you have to take to the movies.

Lorena Marciano: Besides the jokes, I think we're in a moment where, like it or not, privacy would be a part of your development lifecycle. Wherever you want to go, that should stay as your fundamental element, that you need to think about those controls that you want to put in place, that when you're using it, that you're doing it in a thoroughly, sparingly, and proportional way. If you think about it, it's exciting. It requires different skills, legal people working with the project manager, with engineers, and it's an exciting moment where you can come together and extend your skills.

Michelle Dennedy: Yeah, it's cool.

Harvey Jang: Yeah, and I think for me what's exciting is just seeing the change over the past several years and even a changing of the guard among the regulators. Yes, the fear of fines is still there and they have a very big stick ...

Michelle Dennedy: If you're listening, we're still officially afraid of you.

Harvey Jang: They're much more engaging. We want to hear from industry and they want to work together. They actually want you to do privacy right. They don't want to catch you and beat you, they want you to do it correctly. Some of our regulators provide free consulting services. Here's how you organize your program. Here's how you do the data impact assessment. They're actually trying to help their companies do privacy correctly and protect data.

Lorena Marciano: They're trying to understand from us.

Michelle Dennedy: Yeah.

Lorena Marciano: They're trying to understand how our solution works, because as much as they stuff, they would never be able to be stuffed, like Cisco for example, so that's where I think we're playing an important role. It's engaging with them and sharing our knowledge, our technical knowledge to make them understand how our solution works.

Harvey Jang: Just the partnership. We're all in this together and we're going to change the world

Michelle Dennedy: Yeah. I think that's the big thing. It's a shared mission. It's the stories that we tell about ourselves and amongst ourselves and the persona that we want to portray out there. It's all about treating that data protection, privacy, and human right with a really sacred trust. I think that is the heart about my excitement with this as well. I particularly want to thank you guys. I really want to point out starkly: these lawyers are entertaining and funny.

Harvey Jang: We try.

Michelle Dennedy: Well, at least we're funny to ourselves. If you find yourself on a podcast called Privacy Sigma Riders, you're probably one of us and you like them too. To close us out, where can people find you and learn from you and follow you?

Lorena Marciano: We have our blog. Our privacy blog, your blog, our blogs out there. That's where you can find us. You can find us on social media, so LinkedIn and Twitter. They both carry my name.

Michelle Dennedy: How about you, Harvey?

Harvey Jang: I'm on LinkedIn, but for privacy reasons, I'm not on Twitter.

Michelle Dennedy: You know, sometimes it's good to have both ends of the spectrum on a privacy team.

Well, thanks guys. If there's nothing else that I've taken away from today it's that we have vibrant, global and sometimes interchangeable skill sets that makes it really, really helpful. We have people in the Americas. We have people over in EMEAR. We have people over in Asia and we're all starting to come together in a sort of systematic and really respectful way of treating data and thank you guys for moving the whole industry forward and not just here at your day jobs at Cisco.

Harvey Jang: Thanks.

Lorena Marciano: Thank you.

Michelle Dennedy: Thanks for listening to Privacy Sigma Riders, brought to you by the Cisco Security and Trust Team. Special thanks to Kory Westerhold for our theme music. You can find all of our episodes on Trust.Cisco.com or subscribe wherever you listen to podcasts. If you listen on iTunes, please take a moment to review and rate us. To stay ahead of the curve between episodes, follow us on Facebook, LinkedIn, and Twitter. You can find me, Michelle Dennedy, on Twitter @mdennedy. Until next time ...