**Host**

Today we are speaking with Akshay Garkel Partner, Grant Thornton, about data privacy. Akshay is a business leader with about 20 plus years of work experience in information security and cyber security spanning across various geographies, including India, APAC, and Middle East. His areas of expertise, blend cybersecurity business and practice management. Thank you so much for being with us, Akshay.

**Akshay Garkel**

Thank you, Anisha for having me over.

**Host**

Akshay, recently, it was reported that Air India and Domino's Pizza suffered data breaches where sensitive personal data of their customers was leaked over the internet. So, what is data protection and privacy mean for businesses in India?

**Akshay Garkel**

So, we look at data privacy and protection, privacy predominantly, you know, is protecting the personal identifiable information of customers and individuals within various businesses and geographies. When you talk about data protection, data protection is a larger term, it's a bigger term, where essentially, it is not about data protection points within the privacy aspect, where you protect the PII's and the SPDI's but you also protect confidential information of the organization. For example, when you look at, say, for example, important business, business files or critical information like sales protection etc. is a confidential information about a specific business, information about individuals, for example, their name, their age, gender, their preferences, is a private information or personal identifiable information about that individual. Now, what does it mean to businesses in India, it means that lot of information around the individuals have to be protected by businesses, and those individuals could be either employees, individuals from third party ecosystem, or it could be their end customers. As far as data protection is concerned, of course, there is confidential information within every business.

**Host**

Do privacy and data protection always go together?

**Akshay Garkel**

I agree that they do go hand in hand, there would be various aspects of privacy, which would be a part of the overall data protection framework, privacy is something as I mentioned to you, various aspects, right from looking at, take an example of a password, individual's password on the system, that would be a part of the DPIA as well, and at the same time would come under the gamut of data protection too. However, if you look at somebody's name, or financial information, or residential address, or you look at spouse's details, those predominantly would be constituted under the DPIA, of course, various laws between various countries essentially will have different interpretation. You have basically the California act, you have the general data protection regulation in Europe. You have the PIPEDA in Canada, and of course, the India data protection bill which is coming up in India. So, all of these would essentially have their own interpretation, but predominantly, the baseline remains the same.

**Host**

Right. But as of now, as a company, what is my liability? Should there be a breach of my customers data?

**Akshay Garkel**

In terms of the liability again there are two aspects that one needs to understand, while any business basically complies to the Data Protection Act, or the Privacy Act is that, you know, what is the role that they're playing in terms of managing the information are they processor of the information, or are they the controller of the information. Now, if I am liable directly to the regulator to comply to privacy, then I'm accountable directly to those specific fines. Now, each Protection Act essentially has got different liabilities. For example, if you look at the Indian data protection, where what is proposed in the bill, any breach, which essentially constitutes to a PII above the age of 18 and if it is proven that a specific control has not been complied to, then the breach could be anywhere between 2-4% of your global turnover or it could be five crores INR, whichever is higher. The second is if the PII is basically under the age of 18, then essentially the fines are much higher. Now, it will be interesting to see how the Data Protection Authority of India is going to apply rules and learn from various other acts globally.

**Host**

Right, now you just said that data breaches once, you know, the law comes about, could entail a financial penalty for companies and, you know, recently we had this episode of the colonial pipeline in the US where they were hacked and, you know, the company was locked out of its own system, it couldn't, you know, the hackers had gained control and locked them out. And they said, you give us the ransom, otherwise, we will not let you into your own system. And because of that, the pipeline had to shut down, you know, they had to physically shut down the gas pumps, people were stranded without any gas. And, you know, it was a problem in the east coast in the US. Now, how should Indian businesses tackle data privacy and protection related challenges because one thing is your customer's data. The other thing is your own sensitive enterprise data, and when misused can really lead you to completely grow out of charge and hampered.

**Akshay Garkel**

Right absolutely. And if I, before I answer this question, I can just add to that statement, that, you know, there have been instances where for us to basically protect fair amount of information breaches, or protect ourselves from these kinds of ransomware attacks, where the business essentially starts getting locked down and there are operations, which essentially are getting hit, and there is a lot of, you know, reputation loss and financial losses, organizations do need access to information, which also include PII to a considerable level. I can give you some examples where, you know, confidential information has been started, I mean, they confidential information starts getting ported out to personal IDs, and that confidential information may contain employee list, it may contain contractual information, it may contain sales pipelines, it may contain business strategies, right. And from that standpoint, it is a direct or an indirect loss to business and to your question, how do business tackle the challenges? I think it's a multi stage process. The first and foremost is businesses should not wait and they should immediately start planning towards the compliance. Because if you look at the, you know, the ratification of set of controls, it's a holistic coverage. And when you say holistic coverage, it talks about technology. It talks about the processes within the business. And it also talks about the legal framework. Right? So, it is important to start planning today itself. There are a lot of businesses who have operations overseas, and they are complying to the law of the land, because there are a couple of guidelines which are already mature and ratified.

Now, the second is that, you know, it is important to identify gaps and do a self-study within the organization and understand where do we stand. The next step is once you identify the gaps, you basically go ahead and start building a charter and start building a plan in terms of how you're going to implement those gaps, right. And when I talk about implementing the gaps, the gaps essentially as I pointed out earlier, could be either in the process area that means does my business process require a complete reengineering? Now, let me give you an example of business process reengineering, you take an insurance organization, earlier what used to happen was that, you know, you have the end agent coming to your house or you know, connecting with you

as an individual writing a form and from that form, basically taking all your information because you have to subscribe to a policy. So, for that obvious reason, I even need information like your age, your medical records, your health, you know, your spouse's health, your dependents, health and all those information that is all PII, that information now essentially starts getting captured into the system as a next step. And then basically it goes out to the underwriter and the underwriter based on the profile of the customer would essentially, you know, approve the policy. Now, now imagine once the Privacy Act comes into picture, does this process actually require a complete re-engineering? What that means is that, do I need to stop collecting this information? Do I need to make it portal based? Do I need explicit consent right, from Anisha, for example, Anisha can I use your name?

**Host**- to share my data

**Akshay Garkel**

And I will be using this information only in the specific locations for the specific purposes. Tomorrow, Anisha can very comfortably come back and say that Look, Mr. Insurance Company, I want you to forget my information. What does that mean? If, if I forget my information, what does that means, I have to delete all the instances and I need to reconfirm back to Anisha that I have forgotten your information. I don't have any trace or track of that information, except for purposes of law enforcement agencies in case if they ask for it. One more point that I would like to say in terms of how to tackle the challenges, you know, set up your data protection office, that's very, very critical and data protection, when we spoke about data privacy and protection, data protection cannot be a part of the information security teams, data protection has to be an organization wide function. And Information Security should have a dotted line or a connect to data privacy and protect, however data privacy and protection to cut across the organization as an independent function.

**Host**

How is COVID-19 impacting our privacy, like it or not, we are giving out our information because of many reasons, we can't step out or whatever, whatever the reasons. So, how is this impacting our privacy?

**Akshay Garkel**

There was very little time for the businesses to react, and go back to the offices and you know, create a secure environment. Of course, a lot of good attempts was made, and probably, depending on the agility of the organization, depending on the readiness of the organization, various businesses started securing the remote working from home environment, and the remote mobility programs really kicked in. However, during that period, you know, hackers took a lot of advantage. And I have come across a lot, many organizations who've actually gone ahead, I mean, who have basically got compromised and they couldn't even reach to their offices, to basically revive all the, you know, revive all the information, which essentially got either lost, or there was downtime because of the ransomware or there were operational challenges. And because of that business suffered a lot of losses. There were a lot of non-compliances, regulators were questioning them, and so on so forth, so, this is one of the examples where I can tell you that COVID-19 initially how impacted, however, you know, I think the way organizations have today come up, if you look at some of the platforms like you know, without naming them, but few of them, the popular ones, like Microsoft Teams, we have Zoom, we have WebEx, you know we have Blue Jeans**.** They have essentially, you know, the way they have actually created their entire environment, businesses have actually started to look at using them in a longer run perspective.

**Host**

My question is as an individual, where is my privacy now, either I dig my head into the sand like an ostrich and say no, I won't share my data with anyone, but I can't survive like this.

**Akshay Garkel**

If you would, you know, take note that RBI has come up with a Master directions circular, for payment aggregators and for regulated entities. So, the regulated entities like banks, essentially are going to be primarily accountable to make sure that if at all there is breach of information, there is a breach of privacy. And that privacy breach essentially, you know, leads to a situation where somebody's financial information is compromised, then the regulated entity is responsible. And the definition of a regulated industry entity is predominantly banks and financial Institute's. So, having said that, there was a submission by the banks, that if at all that happens, then we need to, if we are responsible and accountable, then we should make sure that the financial information is only stored on our servers, aggregator platforms can only ask for authentication.

**Host**

Yeah, but when I'm shopping on say, shopping on Myntra. I am keying in all 16 digits of my credit card and my CVV number. Now you're saying it's encrypted so people at Myntra cannot see it, is so, I am safe, is this what you saying?

**Akshay Garkel**

Yes, at this point in time Myntra does have the information. But with the new circular and the regulatory directive coming in a very soon Myntra will not be allowed to carry that information and that information will be directly stored with the bank and Myntra will only have a chat with the bank or they will have a connect with the bank at the time of the transaction. And the bank will authorize the transaction stating that this customer I have the credit card details, I have the debit card details. They have enough balance in the account and please process the transaction. That's the way it's going to move forward.

**Host**

Alright, Akshay I also want to talk to you about this recent face-off between social media companies like Facebook and Twitter and the Indian government. What do you make of this entire face-off between the social media giants and the government? Is privacy involved in this entire issue?

**Akshay Garkel**

Again, my view here is that when you look at, you know, some kind of social media companies, one where we are saying that, you know, the users have the right to go ahead and protect their privacy, and then give consent for organizations to use it. Second is that, you know, we are basically going ahead and preaching our own privacy by putting whatever information on social media, and this is purely my view, I feel that, you know, we need to be a little responsible as individuals as well, while there is a fundamental right, the Supreme Court has also given us verdict. But today, you know, if I am essentially going on social media, it is very important for us to basically follow some of the norms, like for example, you know, are you really inviting strangers into your social media and you're allowing them to be friends, number one, number two, are you really sharing a lot of personal information in terms of your locations? When did you check in, where did you check in, your child basically goes to school so which school does he go to, morning he goes here, evening he goes here, again night, you know, you did this, that basically gives a complete trail and tracks for a crime and criminal, you know, activity to happen. So, are we also am I'm not saying that, you know, we don't have the right but again, we need to be a little careful in terms of who we invite?

**Host**

Experts have noticed this trend of youtubers from neighbouring countries sharing content that naturally attracts Indians and Indians who then give away their digital information when subscribing to these channels. So, you know, how do we become smarter? We may not, you know, we may not know that this is not an Indian channel or, you know, people who are collecting our data, may have some other kind of motive.

**Akshay Garkel**

Social media companies should on continuous basis, create that awareness throw out pop ups, make sure that they give the guidelines the way banks give the guidelines to their end customers. And make sure that you know, they are you know, creating an awareness time and again time and again right and keep slowly but gradually keep knocking into the customers or the social media users that, what is their, what is the right mode of ethics in terms of following the laws and the rules? And you'll see that you know, anything which has got religious bias comments, which have got political comments or comments, which can actually create a furore, certain videos, which basically, talk about anti-social elements, all of those get deleted, anything, which is, you know, and if you have the mechanism to report those as well. So today, most of the social media companies have created a reporting mechanism you can report to them, and I have seen most of them generally do take action, and they basically, you know, put that down. So, that is what I would suggest that, from that standpoint, it is important that, you know, we create that level of awareness at all times.

**Host**

Right. What do you think are the best lessons that India can learn from other countries when it comes to data privacy?

**Akshay Garkel**

Banning is not something which we should learn as a country but we should definitely not tolerate extremism. So that is one thing that I would for sure say. Second is that, I'll break this question in two parts. One is India, India for businesses. More at the business standpoint, I would say that regular audits, a lot of regulatory bodies have given enough time for businesses to comply, number two setup a data protection office, it has to be independent function, reporting right up to the board. Number three, is educate and create awareness on the personal identifiable information.

**Host**

That was such an insightful discussion. Thanks, Akshay for your time and talking to us. We really appreciate your efforts. That’s all for this episode of Mrigashira, see you next week with another topic. Till then stay safe and take good care of yourself.