Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 11
Lecture: 33

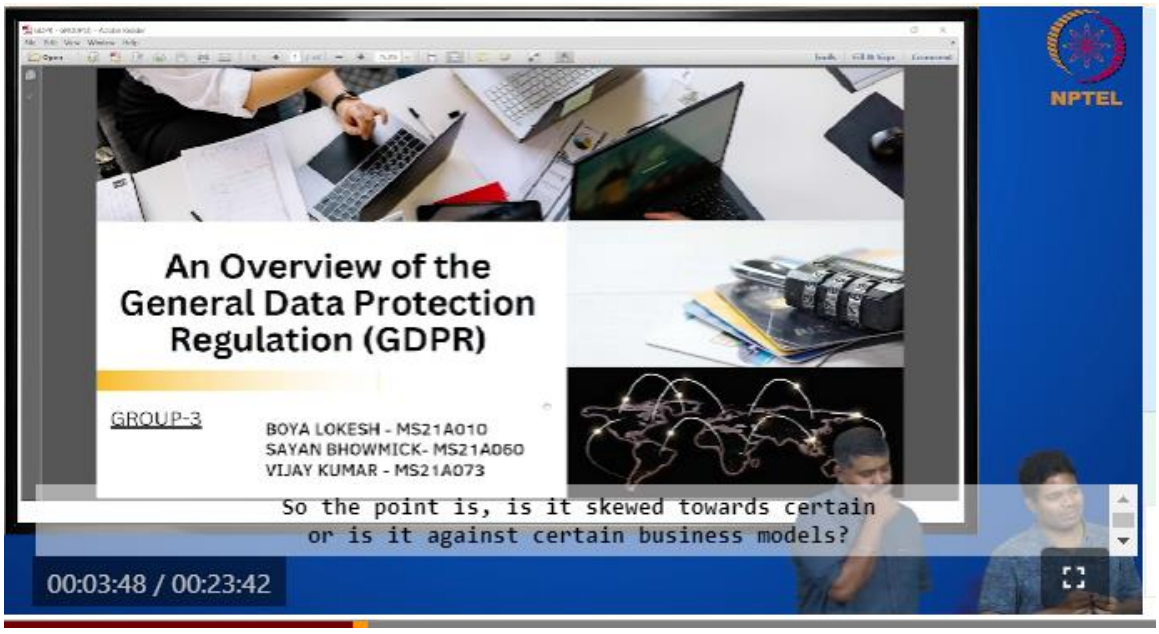
Okay, so that was an excellent overview of GDPR. And of course, you refer to the basic document of GDPR and gave us awareness about GDPR and its legal basis and its implications for organizations based in EU and based outside of EU. And so GDPR was implemented, keeping in mind the interest of individuals predominantly. And post GDPR, you also showed some figures as to what is the impact of GDPR on particularly organizations. And you have repeatedly showed how American firms have been fined. And Europe has been making money by penalty from American companies who actually use data.

So you highlighted Google, Facebook, Amazon, and even Microsoft, whose commentary you presented have been repeatedly fined in EU post GDPR, although they claim they are all set to go etc. So let us also look at the downside of GDPR. So is it bringing a regime where it is against the business interest or business models of certain companies who do business in Europe? Does it sort of affect or adversely affect the value of business that is based on data? So for example, if you look at Google or Facebook, they are top companies of the world today, technology companies, and their business model is based on data.

And if you have a very strict regulatory regime where collection, storage, processing and transfer of data is strictly regulated, is it possible for them to function at all? Because they all depend on advertising industry for their revenues.

And if advertisers do not get information about what people need, that is what they do. That is a value they create for advertisers and that is the source of their revenue. Isn't it going against the business model of certain companies? Isn't it actually against entrepreneurship and innovation? That's my question against GDPR, if you actually make the law so strict. Interestingly I would tell you, in GDPR there are certain countries to which organizations in EU can freely transfer data. They call it expressly permitted countries.

Interestingly, United States is not one of them. You expect USA to be there. USA is not one country where they have said, you have express permission to transfer data. Even India is not there in the list. So countries where there is strict data protection regulation, they allow that.



So the point is, is it skewed towards certain or is it against certain business models? No Sir, because generally a business means they could do in ' n' number of ways, not only using the data, they could promote their business. It means they can not use the personal data and make a call that do you need this product, do you need this service and undermining the privacy of the individual. That can not be done to satisfy the business needs. So that we… But that's a very simplistic argument, I believe. I agree to what your

point is there and yes, to some extent regulations and as they go stricter, they do stifle business.

But then the counterpoint or the counter argument to that is, in case I will just give an example, say there is a mining permit and environmental clearances which are given. If you give it in a blanket manner that everyone has that, you have seen a particular case, one sees a particular, okay here this is not like the lithium has been discovered. So if you give environmental, I have been to that area and all, it is a totally forested area and all those things and now you give that clearance, it will lead to whatever environmental effect which is there. But if you give it a blanket sanction that everyone, anywhere in the country can do the thing, what will it basically lead to? So that is the effect. When you give a blanket sanction, what the GDPR is saying that you have to adhere to these regulations and this should become a norm in the greater good.

Now what the businesses have to do is, they have to adapt to these regulations in the greater good. Yes, it will be stifling to those organizations who don't want to adapt to it or But the negative side of that is what we saw, the recent controversies which are going on, the Facebook controversy. They were called in their own country, the Twitter controversy which is going on, their own officials, those are the negative aspects to it because in the absence of regulation, there will be blatant, there can be or there is likely to be blatant misuse of your… Okay good, I take your argument. So in the Equifax case we discussed, we found at the end, the major issue was accountability. So actually GDPR brings some sort of accountability for the firms, not only those who collect data but also who process data.

It is not that, you know, there is no clarity about what will happen if something goes wrong and what is the penalty, when it has to be reported. Since there is no clear law, people can play around and who is accountable. So there has to be accountability within firms and that has to be established, etc. So in that sense, GDPR brings sort of accountability for individual's data. The other extreme is also not good that it should also encourage business and data privacy as we saw and as we are going to see also, is not an absolute concept and therefore it has to be seen from both sides.

People are willing to share their data, at the same time they don't want data to be abused. So both sides are there. My last point regarding GDPR is that it has certain innovative aspects like privacy by design, privacy by default, suggesting that if you are signing into an account, by default the radio button should be I disagree, not I agree. So if I agree, you know, these are actually called nudges, these are called nudges, you know, so Richard Taylor's idea of nudge. If you say I agree, you tend to agree with that.

So if by default it is I disagree, then you know, it gives you a point to think whether I should agree or not. So it serves as a nudge for, in the interest of the user, that is the point. And by design of course, privacy has to be thought of prior, it should not be an afterthought. So these are actually very innovative ideas in GDPR.

Excellent. But my one point is to comply with GDPR. So firms actually safeguard themselves. Ever since 2018, I see this consent business. So any website particularly associated with Europe, if you go, they immediately bring up the cookie policy. So this is a recent phenomenon since GDPR.

So we use cookies. Can we, you agree with using all cookies or you decline? This is a consent every time you have to give. Almost three options. What do you do actually with them? You agree or you don't agree? Majority agree. You give manage also.

Over here, we are all agreed to because as I said, it is aware, we don't know. Actually again, the difficulty is if you have to go to your settings and change cookies, you don't have all that time. Right. When you are, again, it goes against the human need and gratify. So you're trying to gratify some immediate need and we don't have the time.

So that I agree, again or use all cookies is not serving any purpose. It is only sort of annoyance for individuals. And this topic was discussed in a conference on privacy also in recent, recently. So it is not serving a purpose because consent at the end, we may say every company should take consent from me before they act on my data. And if they start, if so, if so many firms taking, start taking consent by, in this format, you don't have time actually, to read the clauses and agree or disagree.

It doesn't practically work. The consent actually doesn't practically work. Actually Sir, I remember there was a message which was floating in WhatsApp in which one person is complaining to IRCTC. He has put it in their feedback and grievance that whenever I log into your site, it starts showing me a lot of illegal site pictures and all those things. So IRCTC actually replied, "Sorry sir.

" It depends upon which sites you have been constantly visiting and those sites are only being, their ads are being displayed. So it has nothing to do with us. It is everything to do with your surfing habits. So no, it basically brought out that whenever you are visiting all these sites and all, earlier what used to happen was, it used to just take all your information, your browsing habits and everything. Now it has started showing the cookies or no cookies or manage cookies.

This is a difference which has come in. Okay. Yeah. Any other questions? GDPR is

something which has been rolled out for the whole of EU, which comprises various countries, right? And each country may have a different, slightly different interpretation. Some may be biased towards being strict while others may take a more lenient interpretation of same law or wherever there is uncertainty in GDPR.

So how is, how is there an effort to harmonize some of that? GDPR is already harmonized. Like earlier it was not harmonized, earlier like under DPD, the EU member countries could individually interpret it and can have their own laws, could have their own laws. It was only a directive. It was not enforced. But under GDPR it has to be complied.

Like it's uniformly applied across all member states. Unlike DPD which is earlier there, where like member states can have different protocols. In case of breach, they can handle, they can impose penalties in a different way. They can have their own implementation of these things. But now it's uniform across all member states.

Like GDPR only mentions that. It's highly extensive and yeah, unanimously designed. But some companies have a preference to go to Irish regulator than to a Dutch regulator for the same GDPR. Sorry, come again. Some companies have a preference to go to an Irish regulator than to a Dutch regulator for the same GDPR, to clarify interpretation or to ensure that they are compliant. So there must, there would be some difference still there which exists which would be leading to this.

But mostly like after Brexit what happened, UK formulated their own law. But that is more or less compliant with the main existing thing. I mean the DPD or maybe the GDPR. That is derived from mostly the earlier laws that were there. Like GDPR is also derived from mostly DPD and other countries who are like, suppose I am telling about, like UK after Brexit, they implemented their own law which is more or less, you know pretty much similar to what is there in GDPR only.

So like, if countries independently formulate their own law, they have to comply with certain principles. They have to be, you know, they have to resort to certain principles by which they can maintain these privacy and all these things. And like Irish, I didn't like research in detail about that whether there is any different laws in other countries. But as far as UK is concerned, I checked their law. It is more or less similar to like GDPR only.

So that's very common knowledge. Anything else? Is your question about, does GDPR discriminate against certain countries or is it more favourable towards some countries? Is it for data transfer? Is it? It is applied to all member states. GDPR uniformly applies to all member states. But they might be, we did not come across anything of this sort. It has been unanimously adopted and all EU members are, it is not left to countries to decide

now. What is the laid regulations, they are laid? Yes.

There might be cases wherein Ireland might be specifically dealing in some specific service with some specific company outside, that company might also be dealing in the balance of EU countries. So how they are doing if such a case is there, we did not come across that. And how they will, then as you were saying that they will have a slightly more accepting view of breaches or infringement of these privacy laws, then how the Irish or the government or their people are going to reply to, because it is not, when we say Irish firms or this thing, they are ultimately the dealings, we are talking about digital traffic and the regulations pertaining to that, not of manufacturing or thing, basically the digital part of it. And that can be monitored from any point and there would be some central agency or you would have GDPR compliance, that as I mentioned it, they are liable to have a data protection officer in every firm and that is there, mandatory for Ireland also, unless they do not keep such an officer who actually checks it. Then the company is actually taking a very big risk if, even if Ireland is not reporting it.

Some of the other person because it is the European Union, somebody will report it, somebody will bring out these things, It will be slightly far fledged in saying that that the people are all in it and the government is also in it. So be it, let them be. But the company, somebody will report it and they will go in for a very big penalty if such a thing will happen. and actually that people are becoming more and more compliant, organisations. What I heard was initially what this Amazon and all these things happened in the initial time was only because there was a state of flux.

People were, you know traversing that path, wherein people were new to the hybrid mode of working and at that point of time, it was not, Amazon did not do it deliberate, or either Google did not do it deliberately. Before that they did not have such things. it was a open market, open field and when these things came and then people started shifting, work had to be done from home also, from the same people which actually bordered or went into the domain or the realm of privacy of that individual as well as him working for a firm and it was over a public network. So that time they did not have a choice. All these fines and all it did not happen because of a deliberate thing, it was the way it is.

During the COVID pandemic time because that is when this GDPR came into being, into effect. So now I think people are becoming more and more compliant if there are some cases probably, they have already break down. I did not come across any case in our research, any thing like this. In fact GDPR has become the basis or the precursor for many countries, they say 120 countries have already enacted some kind of law and it has become a precursor or the basis for many other countries to form their own regulations. Even countries which are still, you know developing or rising from, as I told Nigeria,

African Union, those countries actually.

So you can take your chances initially with them but maybe once it is fully implemented, I do not think so. So GDPR actually also mentions about third countries. So if you go to the GDPR site and they have specific, you may see it as sort of discriminatory in one sense. So 14 countries they have identified as secure countries to trade data with and other, so these countries seemingly have strict data protection laws. So they have express permission as I said earlier and other countries do not have and therefore it requires for corporations to have contracts, specific contracts which will enable the third country organisations to comply with GDPR.

So that is how this is implemented. So we are a third country in GDPR and we are not in the list of 14, India. So last question, should IIT, Madras in any sense worry about GDPR? The organisation I belong to. Of course you belong to now.

Privacy ? GDPR. That much of information regarding . Anyone can answer. Does it affect us in any department? That's my question. Is there any rules already in place to protect? If it is processing on behalf of any organization, then you come under the purview of GDPR. But if that's not the case, then the pre-existing law that's there in India applies. Unless you are handling data of new individuals or processing data on the other side.

So do we process, do we use or do we process data of individuals from the EU nations? Exchange processes. That's the only thing you are trying to do. Maybe in the research part, there would be collaborators now. What about the speakers who come over here? Yeah, there are start-ups and more importantly, we have joint degree programs with German universities. We have a huge inflow of students from Europe as exchange students who study in IIT Madras say for six months, sometimes one year in joint doctoral programs.

So we do collect, we do store and we do process data of EU citizens or citizens of EU countries. And so, therefore, since we have that data, we should be aware of what GDPR is. So GDPR is basically protect data of its citizens. Now, since we are a third country, we are bound by memorandum of understanding. When we actually have a relationship with another university, we have something called a contract and that contract is called MOU.

So I have read MOUs where we don't have any specific clauses on the protection of private data. So I would say at the moment our awareness is very low. So the point is so long as there is no breach or there is no complaint, things are fine. So the day there is a breach and somebody complains, then all this and somebody goes to court.

How do we know, Sir? There has never been a breach. How do we know? Does it mean that there will not be a breach? Sir, but, so does it mean that we have not had a breach of till now? No, we should be aware. That's the only point I make. Have we had a breach? Have we had a breach? I am not aware. A breach, breaches may have happened, but formal breach, in the sense it became public and it was declared as a breach. As when we were studying regarding the ransomware attack, one piece of information was that all IITs have been breached once or somewhere.

Yeah, yeah, yeah. In the sense many of these databases are actually accessible by students. You know, during our festival, students have access to Dean's students database. I am saying it informally, I am not. So this does happen and we function differently.

But not so the case with Europeans. You know, when I go to teach there, I take a picture with the class in the University of Passau. I have been teaching there for 12 years. I have seen the change in their behaviour. Today, when I take a picture, I have to ask them, can I upload this picture to the website? Only with consent.

If a student says you cannot, I cannot upload. So for, in universities in Germany, they take the consent of every student before their picture goes to the website. These students who are coming, sir, they would have given their consent. But whether we take explicit consent and record it, I do not know. We are not familiar with those practices.

That is what I am trying to emphasise. It may come soon because of the PDP also. India is going for a similar regulation. So we will discuss that in the next class. But we are actually flipping in the sense. We want it to be very strict and when you become too strict, we find that we are losing opportunities.

So, you know, yeah. We will discuss that in the next session. Today we are short of time. So, but we got an awareness of what GDPR does and we will move on to the Indian context in the next class. Thank you very much. .