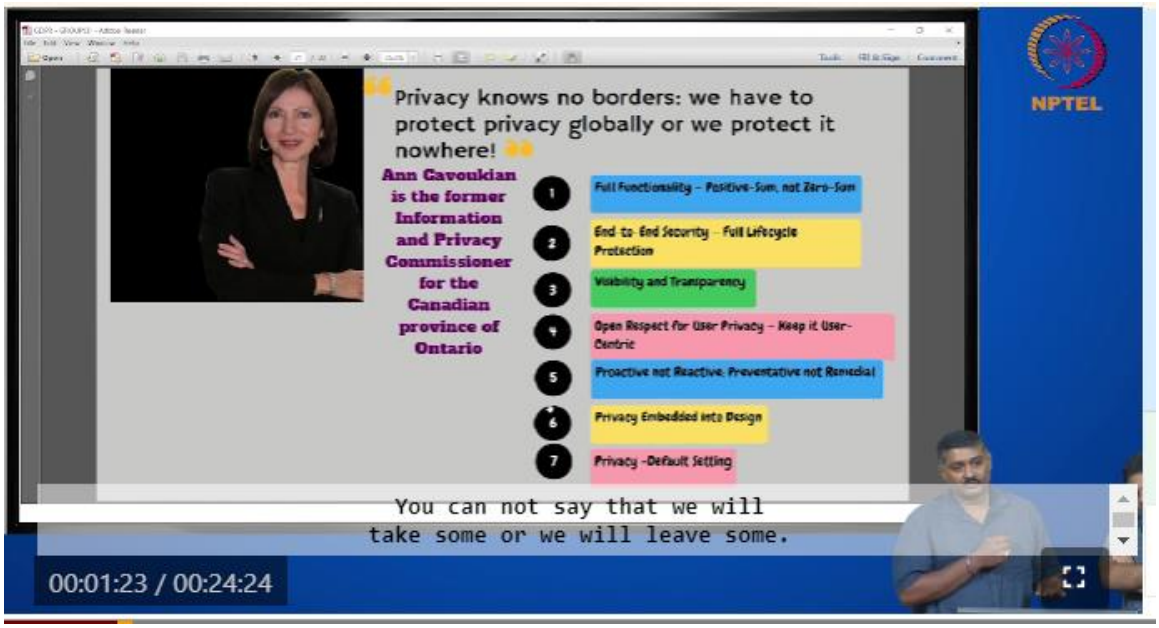
Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 11
Lecture: 32

So, up till now we had a introduction to GDPR and perspectives and comparative analysis. Now, I shall cover few other aspects of GDPR which will also touch upon what was given in the article that is from Microsoft's perspective. So firstly, we should know that who exactly started off with this GDPR. So this lady over there is Ann Cavoukian and she was the former information and privacy commissioner for the Canadian province of Ontario and she is the one who actually laid the foundation for GDPR and as she says that privacy knows no borders, we have to protect privacy globally or we protect it nowhere. She gave seven principles of, based on which the entire GDPR was laid with the foundation. So which says that, the first principle says that it should have full functionality.



Now there is no positive sum or net zero sum, there should be a positive sum and not net zero sum. You can not say that we will take some or we will leave some. It should be either, full privacy should be accorded and it should not be that we will not give full privacy, we will give and take a little bit here and there. So it should have full functionality, it should give the option to the individual user or he should have full control

over his data.

Then end to end security that is full from the beginning itself, from the starting from where the technology or the software or the application starts off towards the full lifecycle of that software or that application and end to end security should be given to the consumer. There should be absolute visibility and transparency in that the customer or the person who is any individual person, he should know what is being taken from. He should not be in ambiguity. He should, there should be clear visibility and transparency from the business, from the company, from the application to the person who is using it and he should be fully aware of what is being taken from him, what is required from him and he should be in control over it. And open respect for user privacy, keep it user centric.

So as previously brought out, the privacy of the user needs to be respected and as Boya had brought out that there are few situations, legitimate, legal, these sort of situations are there wherein this data can be accessed, but then it has to be kept user centric and exact, exactly what is required. So you should not delve right or left of it or you should not move away from your ambit or whatever authority is given and the centricity of the user has to be kept in mind. Whenever anything wrong happens as it was mentioned, like when the COVID thing happened, it was previously mentioned, when the COVID was going on, the businesses actually suffered a lot of cyber attacks. Why? Because majorly they moved on to a hybrid mode, a home working mode. So when that happened, a lot of cyber attacks happened, a lot of data got siphoned off or a lot of user data was jeopardized.

So in that manner, whenever that thing happens, we should not have a reactive approach or rather we should have a proactive approach. Proactive means we should take adequate security measures, antivirus or malware or reporting of the incident, it should be a proactive measure. And rather than going for a remedial, once the action has already happened, we should go for a preventative measure right from the inception stage of the technology or the application or the software or the system which is there. It should already, these preventative measures should be incorporated over it. These were the last two points, privacy embedded into design and privacy default settings also brought up by, as one of which form the basis of the GDPR.

And she says in that privacy should be by design and privacy should be the default setting or should be by default, which basically says or summarizes the entire thing that when a system is being mooted or conceptualized and when it moves, when you finally make it, this privacy aspect should not be an afterthought. And what we, in one of the previous projects also, we said that engineering aspect wherein critical systems need to be isolated and that should, thing should be thought about by the engineers right at the conceptual stage itself. The cyber preventive measure should be thought about in the conceptual

stage, not as an afterthought when the system has been brought online, but before that only, it has to be incorporated right at the design stage. So, the same thing says that this privacy protection aspect should be embedded right at the design stage as a default setting. Henceforth, whatever is being made should cater to this privacy aspect wherein the privacy of the person, the user is protected at all times.

So privacy by design and as a default. So this is what the Microsoft article also starts off and this is the first point which they give is that there is a requirement as per GDPR to have privacy by design and default. Every stage of the development and right from the design services in the process, the system should be compliant or privacy enhancing. It has to be embedded right at the beginning itself and this encompasses IT systems, business practices, the physical design, the network architecture and whatever the strength, how do we decide on the strength of those privacy measures and that will be decided by or rather it should be commensurate to how sensitive your data is. Your data is really sensitive, your medical data, your other data or your legal data or this thing.

So it should be commensurate with the sensitivity of the data whatever protection measures you are incorporating right at the design stage itself. The objective would be that privacy and personal control should be there over one's data by the individual user. Record keeping requirements, that is the second requirement that Microsoft says as per GDPR and we have touched upon this before also that organizations need to maintain a very accurate and up to date record of their processing activities. They just can not be casual about it after the GDPR comes into force and the record should give what is the purpose of the processing, what are the categories of the data which is being processed and the details of the third party who are likely to use it or access that data of the individual person or the business. The organizations to keep records of the data breaches and responses and it is not that you will just leave it at that.

You should also keep a record of any breaches or any attacks and what is the impact of that. That also record has to be kept. Need and practice of data protection impact assessment. This was touched upon before also. So DPI is basically an impact assessment exercise.

Any new processing activity which is incorporated into the business practice will entail a risk and the data protection impact assessment needs to be carried out whenever a new practice or new processing activity is being introduced. So this is what it says. It basically covers when that new activity is there, what is its nature, what is its concept, what is the purpose of the processing which is being mooted right now and what is the likelihood and severity of any potential harm, the threat perception has to be done. And what after a data breach, so what should be as it was touched upon that once any data breach occurs they

are supposed to keep a record of it. But to go a little bit more in data, you have to identify the authorities within 72 hours.

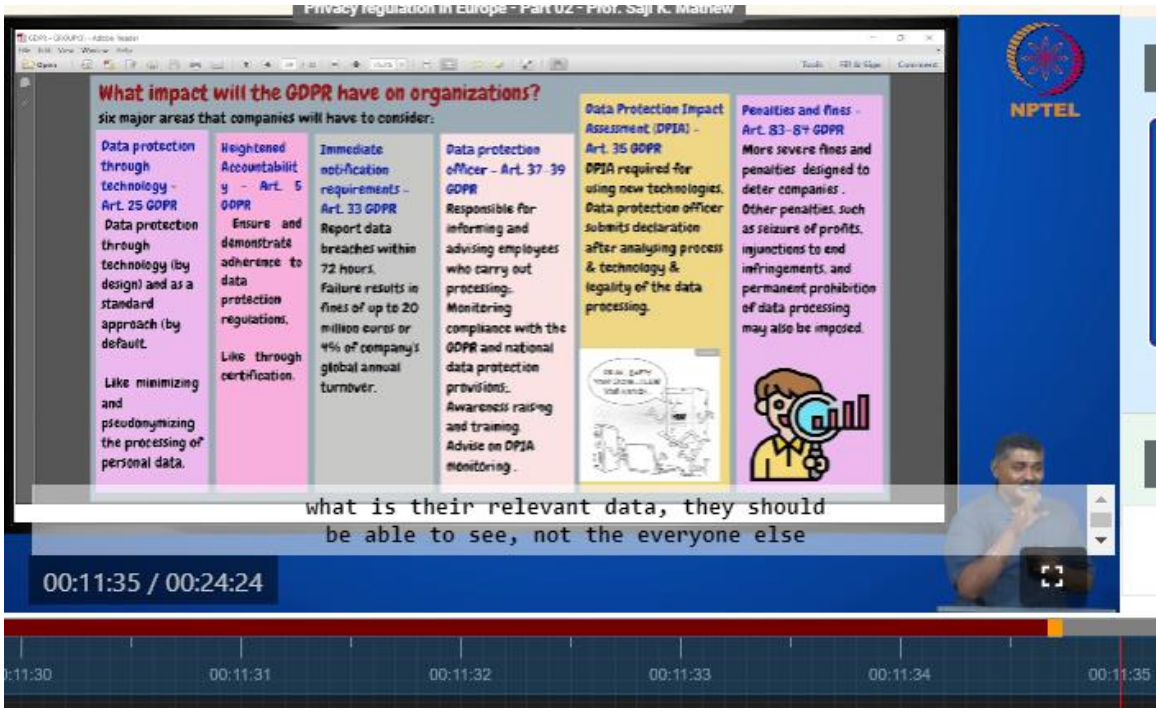
You have to inform the affected individuals also that your data has been compromised and you can't just hide it from the person and adequate technical and organizational measures should be there. They should be incorporated to detect, report and investigate such personal breaches on the personal data. So that is what is action which is supposed to be carried out in GDPR post data breach. And once this data, now EU is not isolated, it is part of the overall global forum in business activities and other things also. And so data transfer prerequisites outside the EU.

So if this data is being transmitted outside for any purpose, for business or industry any activities or travel whichever way for medical. So for countries outside the EU, the recipient country should provide or rather GDPR lays down that it should provide protection in accordance with the GDPR. So lot of people, like last time also we discussed, the outsourcing industry which is there and functioning from India. They do have give lot of heat to the GDPR protocols and the GDPR requirement. And whenever you transfer data to countries that do not provide adequate protection, so they might not have that kind of privacy law, they might not be technologically that ahead.

So what should be done? They should implement appropriate safeguards such as standard contractual clauses, binding corporate rules and all, in order to give at least some semblance of or at par security. Things to know if business vendor processes personal data. So as mentioned in the article and we have already touched upon this the personal, what is an owner or the controller and who is the vendor becomes a processor in this case there is always should be a written agreement and this written agreement should set out the obligations, the responsibilities, what is to be done, what is not to be done and it should comply with the GDPR and the data protection measures and that is what the article says and that Microsoft says that it offers. So in the end Microsoft says that we are perfect for GDPR and basically as far as service is concerned, we give the tools for data protection impact assessment, data mapping, data protection is by design and by default which is the foundation stone of this particular GDPR and they also give cloud data services which have got data encryption and access control and basically goes on to say that they meet all the requirements of GDPR. So once that part was concerned, let us now look at a little bit ahead or outside of the purview of the GDPR.

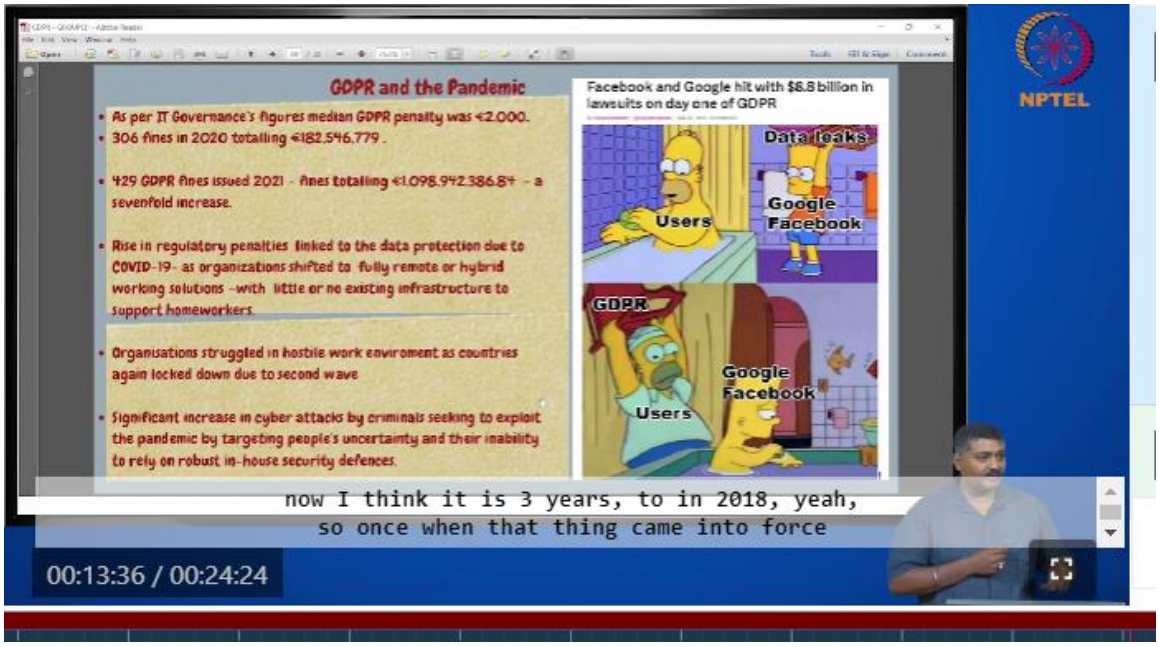
So what impact basically will GDPR have on an organization? What will impact? So as far as the GDPR is concerned, when we talk about the data protection through technologies, one of the articles, it says that it should be as the foundation principle of GDPR, that it should be as a standard approach as a default, like what was brought out,

pseudo-anonymizing the processing of personal data, basically it encrypts your personal data, so that need to know basis the person or the business process of practice which is using it only they should know what is their relevant data, they should be able to see, not the everyone else who can access the data in case of a data breach or anything. So that anonymization should be carried out. Heightened accountability should be there as per one of their articles which basically is true that they should ensure and demonstrate adherence to the regulations of GDPR and something like through a certification, that yes, we are there to it. So this is, these are the requirements which will have to be complied with by an organization. How it makes and how it manifests in an organization or a business organization, how the GDPR will manifest, what will they have to do, so they will also have to immediate notification requirement which we covered that within 72 hours they have to inform, not only that they have been breached but also that the individual, you have been breached.



So that is one of the requirements Data protection officer has to be nominated, who will basically be responsible for advising awareness training of the employees and monitoring that all compliance is being monitored. So this particular officer has to be there in an organization. This is one of the requirements as GDPR manifests itself in an organization and DPIA, the impact assessment, any new thing which is being introduced into the organization, any new process and impact assessment has to be carried out and this will be under the purview of the data protection officer. He has to carry out and check it that

the impact of this, what all safeguards are there, is it is the design and default clause already incorporated or not. Penalties and fines, has brought out very severe fines, more severe fines and penalties are designed to deter companies and there are other profit like other penalties like seizure of profits injunctions.



So it can do substantial harm which the company needs to be alive to or the organization needs to be alive to. So as it was mentioned that Amazon had the largest penalty which was there and Google had it and British Airways, as he brought out, so at that point of time when GDPR came into force now I think it is 3 years, to in 2018, yeah, so once when that thing came into force by 2020 when the figures which was given was that the minimum penalty was 2000 euros and 306 fines were levied in 2020 which as the figure shows in euros amounted to and about by the time it was 2021, it amounted to 429 and the money as you can see, that it was substantial it was a seven fold increase. So this rise in regulatory penalties linked to data protection due to COVID-19 was basically because people were switching from, the organizations were not prepared to go into that hybrid working mode. They and when they, when the people switched over to working from home and the hybrid mode, so it was not the organization's fault also. It was the people's fault also because when they started working from home, the home environment did not have that kind of safeguards or data protection safeguards already there and that is where number of breaches occurred because it was the time when there was substantial cyber attacks which were also being carried out.

And naturally if you're working from home and that kind of data protection safeguards

are not there in your personal PC or personal computer or even in the public network when you are using, so you're likely to have a lot of cyber attacks in which because it is business there is a lot of business intelligence and counter intelligence and people want to siphon of information. So that is how it happened. Now conclusions, about way forward for GDPR. Now we know that, we should know that this privacy aspect, the people are going very very sentimental and very concerned about it and it is here to stay. So privacy was not the norm but going forward privacy is going to be the new normal.

Customers will expect it. Authorities will check it and finally the corporates will do it. They are already at it. There will be more automation, the automation part is not going to reduce. It is likely to grow only, the only thing is, what the aspect which we talked about is, by that is privacy by design, privacy by default and not as an afterthought. For organizations, they are likely, they will definitely mature and they are still in the early stages or the initial stages or nascent stages of this regulation compliance and more and more regulations are similarly privacy laws are likely to or already there almost hundred and twenty countries have enacted their own privacy laws and it is likely to increase, the severity is likely to increase, the penalties are likely to increase.

The privacy will actually become a brand differentiator and in terms of winning more clients and as one of the study shows that 82% of organizations view privacy certifications and privacy shield as a buying factor. People are concerned about that. People will go for any product or any service, anything based on this privacy thing. It is going to be a one of the key factors to corner a market in the days to come. In short like it or not, GDPR such like and privacy laws are here to stay and we can keep debating that this is not there and whether it is not fair, whether the penalties are not fair or hybrid home working but it is better to take a more practical approach and comply and have a more long term perspective on privacy laws.

Just to touch upon what I had told, almost hundred and twenty countries, I could not put all the countries, some of the countries which are put. So Australia the privacy amendment bill which was an amendment to the Australia Privacy Act came into effect February 2018 and if we look at Brazil, that also has this LGPD, which is modelled on GDPR with lesser, less penalties the penalty degree is lesser but it is already there and definitely it will get modified. Canada has also implemented a digital charter implementation act. The People's Republic of China has passed a personal information protection law. India, our country has already introduced this bill which is the personal data protection bill and companies all over India, already they are starting gearing up to, they have started preparing for it.

Israel has a Japan's act on protection of personal information was amended and now applies to both foreign and domestic companies and which process the data of Japanese

citizens. Companies located outside of Japan will also now be subject to strict guidelines and other countries like Nigeria which are part of the African Union, they adopted a resolution in 2014 and most of the African Union countries are going by that resolution and they already started enacting their privacy law. So even in countries where their technology is still at the nascent or a little bit more mature than nascent state, they are also going in for this privacy laws and the reference for this data is already given down below and with this we come to the end of our presentation. Actually all these rules, regulation, directions, they are very good and very comprehensive and in detail but where we are failing actually, that is the implementation part.

That is the real challenge. On one side, you know we have this, our rights and we take it as absolute rights and no one actually speaks of the responsibilities. So again in the implementation part, what are the real gaps at the organization level or the national level, international level or the individual levels and how we do this uniformity and standardization especially at the global level ? So like as different India also Sir, mentioned that they are, you know they are preparing one law which is, you know which will take care of these data security approaches. Israel, Japan all these nations are forming them. So after that I feel that, yes it will take some time. But if these laws are being very strict and you know they are imposing fine, heavy fine safety penalties.

So I guess it will be gradually implemented, like if these are very strict and all then the organization have to be compliant with all of this. So Sir, actually that is a good question, though slightly out of GDPR aspect but yes, it is a relevant question, in coming, in today's day. What we have to focus on is that all countries are not the same, culture is not the same, population is not the same, infrastructure is not the same. So what you, when we say that the GDPR is based on two founding principles that is privacy by design and privacy by default, to have such a thing you need to have that manufacturing capability with you. If something is being manufacturing outside and you are just importing it, you can't have your say on it.

So yes, stricter penalties and all those things, like we are also doing that. In fact we don't have a 4% penalty, our penalty has been moved to almost 5% of the global turnover, that is what is being moved. But you have to understand just like US, in which each state has its own laws and they work independently or more or less independently from the federal government, each state has been enacting laws over there also. So how it is implemented will depend upon the demography, the culture of the country. For a country like, for a player for some something, like EU where in number of countries are there, the population is very less, the infrastructure is already developed, it is easy to or rather more or less comparatively easy, to implement all these things and when majority of your exports are going to EU, they have the say.

Do this, do this, don't do this, but if you are a net importer of things you don't have that kind of leverage on people. So it has got broad ramifications. It has got lot of other linkages which has to be done. One thing which can be done to actually have a good private look. In our country also, rampant use of Facebook and all that, how many people are actually worried about cookies and all ? You just press okay, majority of us, at least the site will open.

Now only these laws and things are coming into force and now only the younger generation are getting more alive to these sort of things, malware, cyber attacks and all. These people are now thinking about their private information going off. Now cyber attacks are targeting the Indian personal data and all. So as you, as we continue to grow to that level, once this rational, once this knowledge or enlightenment comes that privacy laws are important, right from the school education stage and the younger generation, naturally more the laws which are, which have been made will have more acceptability, will have actually, will actually achieve what they are meant to and once I as I said, that number, post this GDPR, number of countries have enacted this laws. Once all the countries have some kind of law, every country will have different law but more or less somewhere that common ground will be found and that would basically form the bulwark of what, as what said how will be plug in the gaps.

So that would form the bulwark and of course, continued education and awareness of the people who are actually the people, the main characters in this entire privacy laws and this ignition game is, are the people who are, who will plug these loopholes, not organization or businesses it is the people, an aware person.