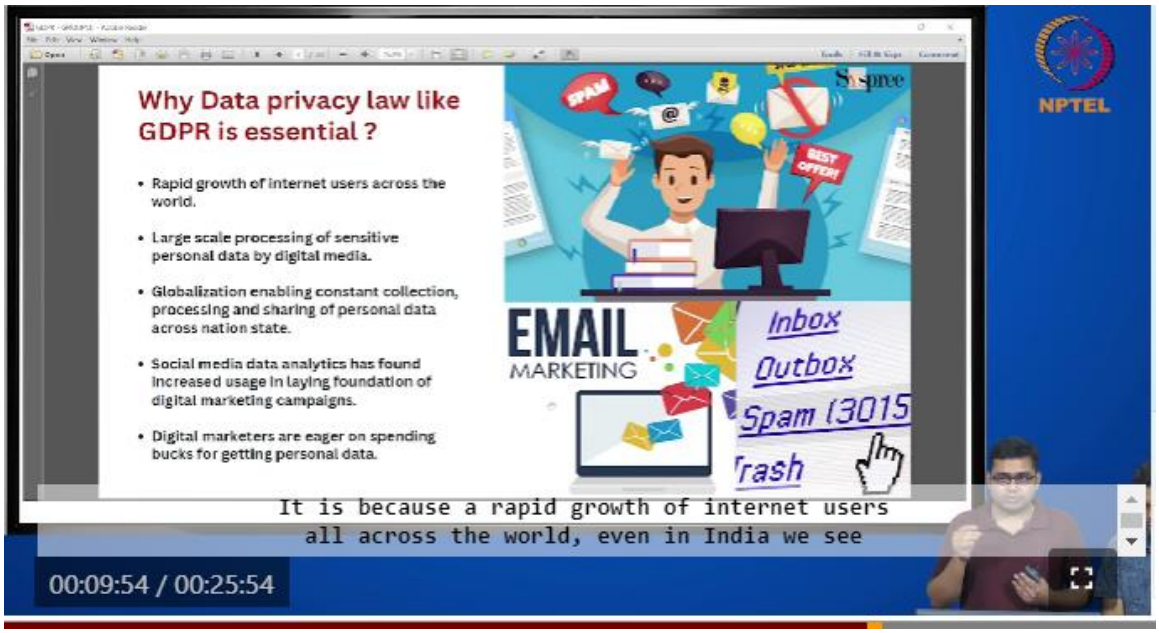
Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 11
Lecture: 31

Good morning, so we are starting the eleventh session of Cybersecurity and Privacy course and we have been exploring the landscape of data protection regulations and we generally looked at what is the need for regulation and we found that data privacy or individual's need to protect one's private data from exploitation is a basic need. We also saw that it is not just the individual and individual's data but there are other stakeholders involved in the process of collecting, storing and processing individual data. And therefore there are multiple interests, multiple stakeholders and multiple interests. For example, data collectors want to use personal data for certain objectives. So it could be for business, it could be for governments but they need your data. At the same time individuals have a concern for their private data, concern for information privacy.

So this seems to be conflicting objectives and therefore there is a need for regulation to balance, to bring a fair balance among the interest of multiple stakeholders. And in the absence of regulation it can actually move towards the interest of certain dominant players and we know that what, that is what happens in industry and that is where the and that is where the government needs to come in. And cases after cases which we discussed showed the need for tightening regulation in the, in the domain of data privacy and we also noticed

that data privacy and security are very much related. It is for organization, it is the responsibility of organizations to ensure data is protected from breaches or unauthorized access.



So therefore need for security, given the value of these data or the privacy associated with this data. Today there is a separate virtual world that is coming up, you must be aware of the Meta, the world of the Meta. So one interesting fact about the Meta is that if you go to Meta, any of the Meta sites there are many, you do not need a real world identity there. One of my PhD students did a short project on the Meta and in particular about information privacy in the Meta. So what we found was that in the Meta, number one you do not need a real world identity.

What that means is that, it is a separate world, it is a separate planet, it is like going to a altogether different space where nothing in this world you have to carry there. So not your name, not your email id, not your cell phone number, not your date of birth, it is like whatever you want to be, you want, you aspire to be or whatever your aspirations are, you can create that you, there in the Meta world. So there actually people hang around, you create, you call your name whatever you want to call yourself and then you can hang around the Meta world and meet with people, play games, have fun, engage in trade and so many activities. Well, we just found that that world is not regulated yet. There is no regulation, you can do anything there.

So it is still coming up, it is in the stage of early evolution, we have to watch and wait

what problems it may create in future. But we are concerned about data privacy in the real world because there are real persons and real world identities, your data is associated with a self, an individual, a human being. So the value of the self and autonomy of the self etc are at the core when it comes to data privacy. If that does not matter in a virtual world it is fine, we see that it is, you know, it is just open. But as of today in the real world we see data protection is a real issue.

So, what we have done so far is we have discussed a few cases which actually took place in the United States, for example the Target Corporation, We Googled You and Equifax in the previous session. This all pertains to North America, in particular to the United States and these cases showed at the end when a data breach happened, the law did not have the teeth to deal with some of the specific issues. After a breach happens, there are guidelines or there are laws, state wide laws and also nationwide laws as to how companies should collect, store and process data. So those guidelines like the Federal Trade Commission, FTC guidelines and for healthcare data you showed that there is something called HIPAA which is basically to protect healthcare data and for children, you know, to prevent child abuse there are specific regulations that pertains to children and their data. So for different categories there are data protection laws in the United States but there is no overarching regulation that actually provides for protection and safeguard from end to end, not just for prevention but also post event, you know, what should be done.

For example, what is the duration within which a data breach should be reported? We found that that was an issue because there was no specific rule regarding that. And what should be the penalty on data collectors or data processors who would actually collect and process your data? There is no specific guideline on what should be the penalty. So that is what I said, the laws lack the teeth or law enforcement oftentimes is difficult and it also varies between states. So that is the situation in the United States when we actually look at data privacy regulation. So now, subsequently today we are going to see what is the state of affairs in the European Union, predominantly in Europe, excepting of course UK.

And so we will explore the new, fairly new regulation which came into existence in May 2018 and till that time that was a directive or a guideline, just like the FIPS guideline, Fair Information Practices guideline in the United States. There was a guideline in the European Union but it became a law in 2018 and that is a landmark, that is a big change in the world of data privacy. And all over the world there is an increasing concern about the need for protecting private data and that is actually the theme of GDPR. Actually I started this course also around the same time when privacy was becoming a global issue, so in many parts of the world. So Cybersecurity and Privacy.

So it is in that context, so we will focus intently on GDPR today and subsequently I will

give a background and an introduction to a data protection initiative in our country, India and that we will discuss in the next class in more detail. So I hand over the session to the next group to present about GDPR and then we will take it from there. So good morning everyone present, today we group 3, shall be giving an overview of the General Data Protection Regulation which is a more stricter privacy law that has been implemented in EU recently. So as we see that statistics as of January 2023 reveals that 4.76 billion global users has been using social media, like it is 59.

4% of the entire global population and as we see that since 2016 it has been increasing at a rampant rate. While in 2016 it was 2.31 billion, in 2021 it has reached 4.2 billion and by the projection it is supposed to reach approximately 6 billion by 2027. So now why a data privacy law like GDPR in this context becomes essential? It is because a rapid growth of internet users all across the world, even in India we see that internet penetration has been increasing at a rapid rate since 2020.

Now these digital media that the people are using, are processing a large amount of sensitive personal data and also in the context of globalization, we see that the personal data that is being collected or being shared across nation state. Also with the evolution of digital marketing like email marketing, social media marketing and other variants of marketing, we see that the firms are looking after, spending more and more bucks for getting this personal data. So now what is GDPR? GDPR basically stands for General Data Protection Regulation. Now earlier it was DPD that is which was implemented in the year 1995, it was basically a directive, not a law. What used to happen that EU member states could individually just refer this document and could individually implement their own laws.

It was not uniformly enforced but what happened with the advent of digital media and social media, with the advent of digitalization, it was felt that a comprehensive law was necessary to be implemented. So in the year 2016 this data privacy law named GDPR was implemented and it was enforced in the year 2018. Now where is GDPR applicable? GDPR is applicable for all EU member states and all the establishments which are there in EU member states or it is applicable to any organization which is processing data of individuals who are residing in EU. Now GDPR is basically concerned with the storage, processing and sharing of personal data. Personal data means any data which can identify an individual on its own or in conjunction with other.

So apart from this name, physical address, email id which are simple data that can identify an individual, apart from that indirect data like employee information, database, biometric data, retina scan, fingerprint. These indirect kind of data also in conjunction with other data can identify an individual so they also come under the purview of personal data.

Now the question is whether GDPR applied to organization who are indirectly processing the data. As we will see later that there are two kind of organization, one is controller which directly owns the personal data and another is processor who are not directly owning but controllers are handing over that particular data for processing purpose. Earlier under DPD, the controllers were only held responsible but now controllers and processors are both responsible for the security of the data.

There are six underlying principles for GDPR. First comes lawfulness, fairness and transparency. So the organizations which are coming under the purview of GDPR should maintain the fairness and transparency while they are processing the data. So the individuals must have a very clear idea how their data is being used. Purpose limitation, so the data must be used for specified explicit and legitimate purpose, the purpose must be limited and that should be known to the individual.

Minimizing the collection of personal data means only store that data which is adequate and relevant for the processing purpose, not excess data. Then data accuracy, so the organization has to maintain accurate data of the individuals. If it is not accurate then data subjects have the right to get it modified, corrected or may be completely erased and if that does not happen, the data subjects have right to restrict the processing of the data. Limiting the data storage, so when the purpose is served, you do not need to store the data anymore, you can delete it, you do not need to retain that anymore. Then again confidentiality, security and integrity, it is basically the CIA compliance that we already studied in our previous classes, maintaining the confidentiality of the data, security and

integrity.

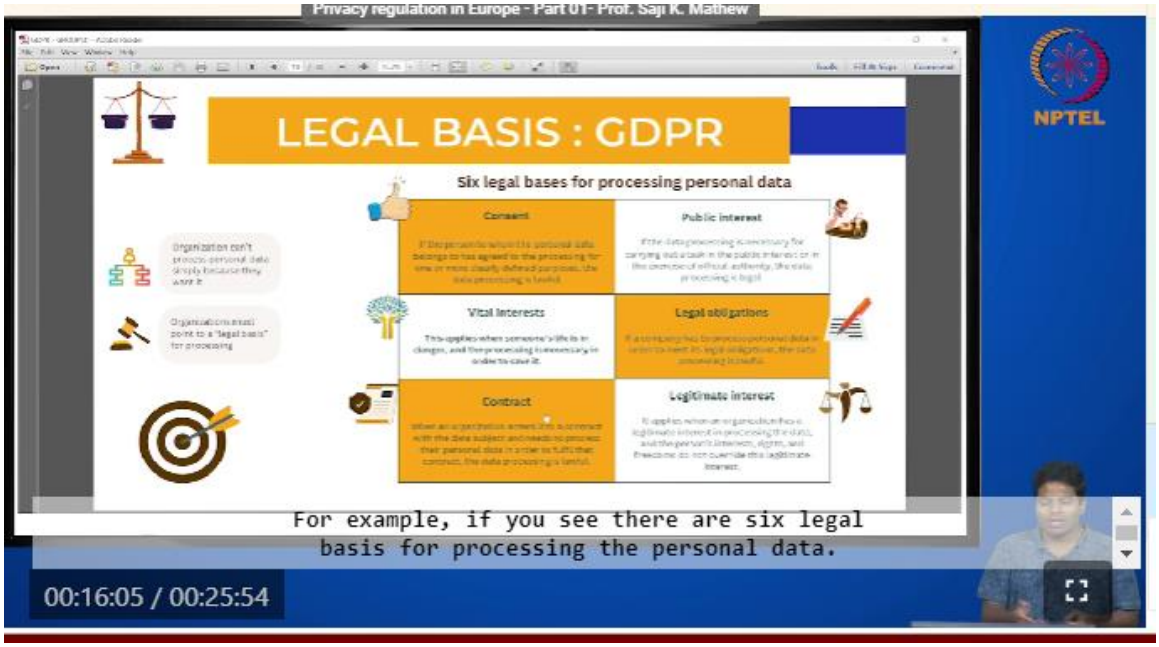
Now I will hand over to Boya for other aspects of GDPR we discussed. Generally there will be non-compliance of GDPR, sometimes it happens intentionally, sometimes it happens unintentional. Means organization may not be knowing the clear policies of GDPR means, how it is going, what are the requirements, still there are some of the organization who does not know the clear policies of GDPR and sometimes it is due to the external cyber threats. Whatever may be the reasons, there will be strict consequences for the non-compliance of GDPR. If you see there is a fine of a maximum of 20 million euros or 4 percent of total global annual revenue, so whichever is higher, they could go with that.

And sometimes it will empower consumers to initiate a civil litigation against the organization that breaches the GDPR. Here are some of the examples. Amazon was fined around 780 million dollars for using the user's data without their consent and this is the largest fine till date. And in case of WhatsApp, it is fine for unclear privacy policies and Google, because Google here it is a means they did not provide the easy way of refusing the cookies, so it was fine for that. And in case of British Airways, it is not because of the, means they did not do intentionally, but due to some cyber attack, there is a breach of around 4 lakhs of customer data.

Due to these reasons, British Airways was fined for that. And transparency, means previously before the implementation of GDPR, organization used to process the data as if they want it. But after the implementation of GDPR, they cannot do it. They have to disclose the purpose of why they are processing such data of the users. And they need to tell the users how long it will be stored and with whom it will be shared.

So, after the implementation of GDPR, transparency came into picture. And there is a legal basis for processing the personal data. Means they cannot process the data because they want it. There is some legal basis. For example, if you see there are six legal basis for processing the personal data.

First one is consent. Means user has to provide the approval. For example, a user enters into an online website and he will enable some check box to receive some management notifications or marketing mails. Here the user is providing the approval for that particular website in order to use their personal data to receive that mail notifications or marketing mails, anything. And vital interest. Suppose if a car accident happens and this person has been taken to the hospital.



In that case, the doctors can use his personal medical records in order to save his life. This is related to vital interest. And contract. Suppose if a user enters online and purchase some goods and he enters a contract with the organization that these goods has to be delivered to that particular place. So, in this context, the organization is a, means has the legal right to process the personal data in order to deliver that particular goods to the user.

And next is public interest. Suppose if a crime happens and the user has witnessed that particular crime, then the investigator authority can use that particular individual who has witnessed the crime, his personal details for further investigation. And legal obligations. Generally financial institutions like banks, any other institution used to perform KYC verification for the anti-money laundering compliance. So in this case, they used to process means, process the client data for the AML complaints. In such a case, processing of client's data is not illegal.

It is totally legal. And legitimate interest. Suppose if a person wants to apply for a job and he has uploaded a resume on a particular website and a recruitment agency used that resume to send it to the clients. Means that this person is capable of doing this job. So, in this context, it is legal for processing the user's data. And these are some of the key terms with respect to GDPR.

First one is controller. Controller means it is a person or authority who will determine the means and purposes of processing personal data. And the next one is processor, who will act on behalf of the controller. And personal data is, as we already discussed, it is

totally related to a identified or identifiable person like name, age, gender, whatever may be the details of a particular person. And processing. Processing means the kind of operation that we perform on a user data.

And pseudonymization means, instead of using the original data, it is replaced with a artificial data. This is nothing but pseudonymization. And security. With respect to security, GDPR does not formulate any measures that have to be taken in order to protect the data. It is up to the organization that they can use based on their severity of the data.

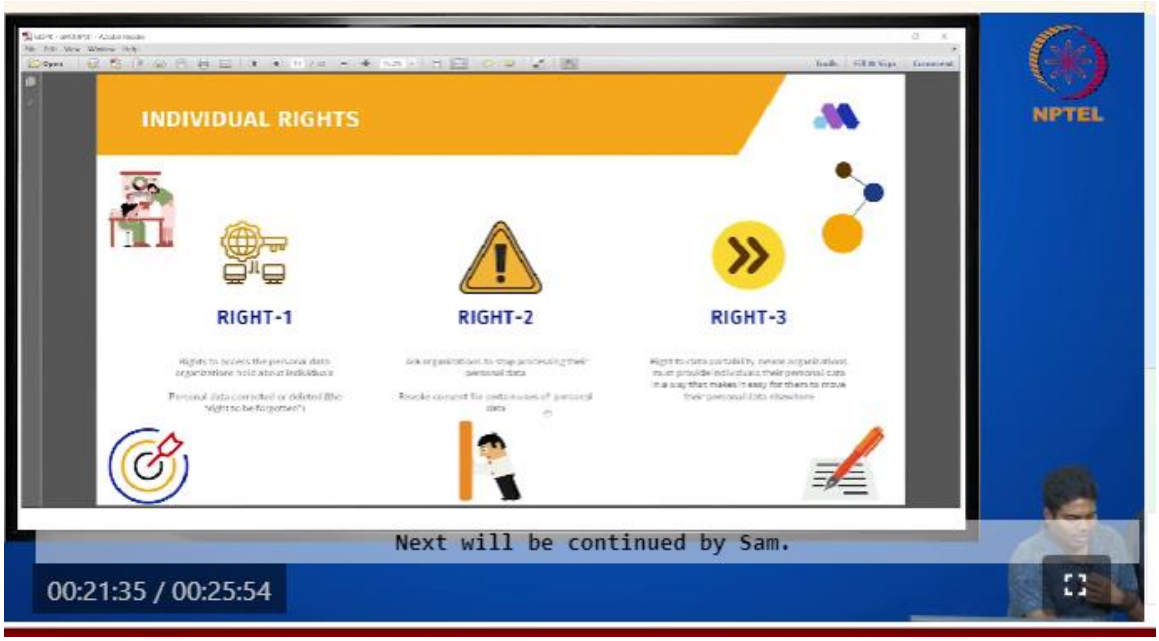
These are some of the security controls like identity and access management. Generally in usual organizations, earlier it used to be like that all the people may be having access to the important information systems. But as there is a lot of data breach, now they are limiting that access to only particular users who require that job function to be done. And data loss prevention. These are the measures that has been taken in order to prevent the loss of data.

If there is any non-compliance, then the processor or controller will be held liable for that non-compliance. Incident response plan means, it is a step by step processor for reporting and mitigating data breaches. And security access service edge means, nowadays before the pandemic, during the pandemic, usually we have completely shifted to work from home option. During that time security, there is a more threat to security or a data breach. In that case, handling this, complying to the GDPR is bit complex.

And after the pandemic also, now we are moving to the hybrid mode, means some days we are working from home, some days we are going to office. In that case, meeting the compliance of GDPR is bit hectic. So, during that situation we could employ these service access, secure access service edge will deploy security protocols to the remote location. And these are some of the requirements as we discussed that data subject rights, means, user can ask for the correction or any changes into the data. Coming to limitations of purpose, data and storage is, he could ask the organization to delete particular aspects of data and consent is nothing but approval.

Data protection officer means, whenever now it is mandatory to employ data protection officer in order to meet the compliance and take care of everything related to the GDPR, awareness and training. There are some sessions usually organization conduct in order to train and train the employees with respect to the requirements of the GDPR. And these are the individual rights, apart from asking that organizations providing why they are using their personal data, individuals also has certain rights that they could ask the organization to delete their personal data or to stop browsing their personal data or to edit

the personal data. And they could also ask the organization to port the data to the some other places, like that they individuals has some particular rights with respect to GDPR.



Next will be continued by Sam. Yeah, so, rights and requirements are already discussed, but still like, we need to say what are the, we need to discuss what are the differences between GDPR and the earlier law, that was earlier directive that was there. So what are the key changes? First, the personal data has been redefined. Earlier personal data was defined only those data which could directly identify that particular person, like name, physical address, phone number, email, but now the scope has been broadened not only like the direct data that identifies a particular person. If there is any data, that in conjunction with another data can individual, can identify that particular individual, that also comes under personal data. Now IP address, mobile device identifier, geolocation data, fingerprints, they cannot directly identify a person, but if some other data is available in conjunction with that, it can also identify that particular person.

So now under GDPR, these data also come under personal data. Earlier this, rights of like opt-in and consent was not enforced in that way in DPD, but under GDPR, the organizations are required to provide explanation of why they are using this data and also by virtue of it, they are supposed to secure the opt-in and consent for the processing of the personal data. And since GDPR empowers the individual, they have given some rights, like right to access the data, right to know how the data is being used, right to get the data erased and right to restrict the processing also. Earlier under DPD only the data controllers organization that is directly, you know, accountable for the data, was held responsible if

data security breach used to happen, but now under GDPR the processor and controller, actually this point we have already discussed. Now, the controller and processor are jointly responsible and for this purpose the processors are now supposed to enter into a contract with the data controllers where their responsibility pertaining to the data security will be discussed and will be held, I mean, will be mentioned in the contract.

GDPR also mandates that you have to appoint a data protection officer. It can be an independent, you know, executive or maybe the executive of a particular firm, will be serving as a central point of contact, regarding, you know, regarding the implementation and whether compliance of the personal data regarding security and all these are maintained or not. This kind of contact will be, through this particular person, data protection officer. Now, the data protection impact assessment or DPIA assessment has been made mandatory for high risk project. Earlier it was not mandatory under DPD, but under GDPR when you are taking up high risk project where you are working with sensitive personal data or you are handling data on a large scale or you are trying to profile a vulnerable section or vulnerable person.

So, in that case, this protection impact, data protection impact assessment has been made mandatory. So, by DPIA we identify the probable risks and their mitigation plan. DPIA, basically a project specific assessment. It is not an organization, it is not a generic evaluation of an organization and basically it ensures that GDPR compliance is maintained as well as data protection, data privacy by design is also implemented into the new projects. Now the penalties and the data breach protocols has been more uniformly implemented as compared to DPD in GDPR.

Earlier what used to happen, EU member countries, because it was a directive not an, not a law, so it was not enforced properly and EU member countries were allowed to adopt different protocols in case of data breach. But now, under GDPR all the member countries are supposed to notify the data subjects that yes, a data breach has happened and that has to be notified within a span of 72 hours. Also the fines have become more heftier and, like you have to pay, a figure of 20 million euros or 4 percent of the global turnover which is, whichever is higher. Now, the next, part will be explained by Vijay.