

# Online Privacy

## Professor Ponnuram Kumaraguru

### Privacy laws and regulations (Part-II)

(Refer Slide Time: 0:17)

Personal Data Protection Bill, 2019  
2019-2022 at 9:51 AM

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY  
HYDRABAD

As introduced in Lok Sabha

**BILL No. 373 of 2019**


**THE PERSONAL DATA PROTECTION BILL, 2019**

ARRANGEMENT OF CLAUSES

CLAUSES CHAPTER I  
Preliminary

1. Short title and commencement.
2. Application of Act to processing of personal data.
3. Definitions.

CHAPTER II  
Objective of Data Protection



1. Short title and commencement.

2. Application of Act to processing of personal data.

3. Definitions.

CHAPTER II  
Objective of Data Protection

4. Prohibition of processing of personal data.
5. Limitation on purpose of processing of personal data.
6. Limitation on collection of personal data.
7. Requirement of notice for collection or processing of personal data.
8. Quality of personal data processed.
9. Restriction on retention of personal data.
10. Accountability of data fiduciary.
11. Consent necessary for processing of personal data.


CHAPTER III  
Grounds for processing of personal data without consent

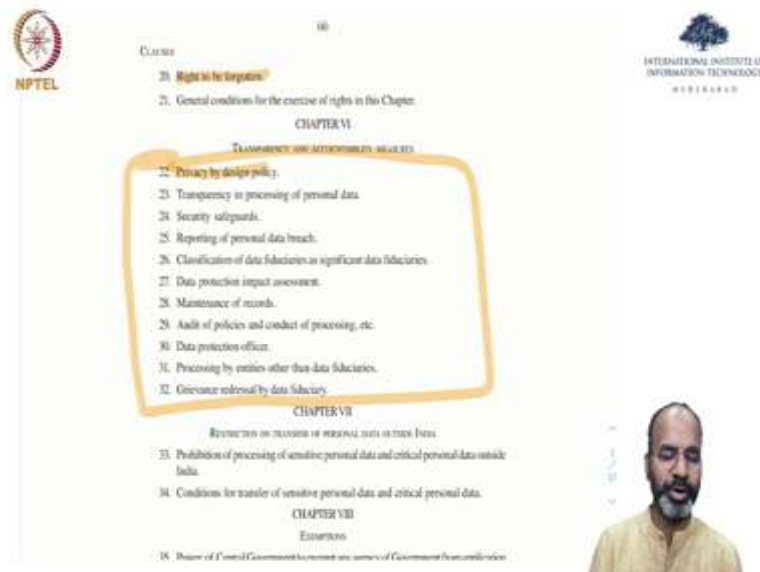
12. **Grounds for processing of personal data without consent in certain cases.**
13. Processing of personal data necessary for purposes related to employment, etc.
14. Processing of personal data for other reasonable purposes.
15. Categorisation of personal data as sensitive personal data.

CHAPTER IV  
Personal Data and Sensitive Personal Data of Children

16. Processing of personal data and sensitive personal data of children.

CHAPTER V





So, now let us look at Personal Data Production Bill. So this is going to be slightly longer, slightly detailed also, so let us go slowly on this because this is under discussion right now, and it is yet to become, yet to become an act so the way, the draft is produced, draft becomes a bill and then revisions goes in the bill and then the bill gets converted into an act, that is when it can be implemented.

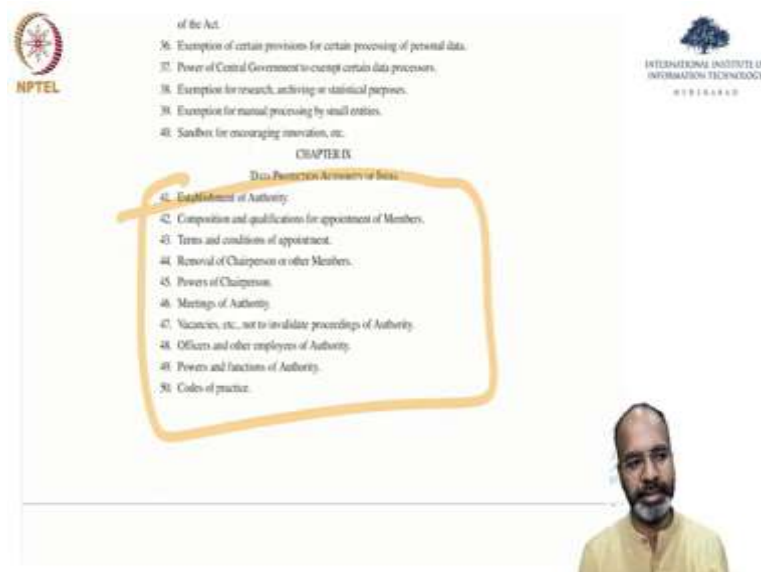
When it is a draft or a bill it is not, it does not really have any powers for it to be used, there is no mandatory requirement if it is not an Act. So, what we are going to look at is the PDP Bill so to say, 2019 is what it was presented. First let us look at what are the aspects of it, we look again. Please remember, it is a 57-page document, very, very legal-ish. I think it will be extremely hard for us to go through all of this as part of this class.

It will probably take multiple weeks of content for it, but my interest is to show you that these things exist and how these things have been implemented, which you can actually use it in your own context. Obligations for data fiduciary, again we look at the definition of fiduciary, data processor, so who has access to the information, prohibition of processing of personal data, limitation of purpose, limitation on collection, requirement for notice, quality of personal data, restriction on retention of personal data, accountability and concern.

So if you look at it some of these words we have already seen in different, different contexts for the class. It is written as part of this bill itself. Then grounds for processing of personal data without concern, in what context can people actually process the data, collect the data and process the data, without having consent for the data. Right to be Forgotten, I think these things have, Right to be Forgotten, it is all very very advanced in Europe right now.

But in India we are just catching up on these topics. Privacy by design, transparency, security safeguards, reporting of personal breach, classification of data fiduciary, data protection impact assessment, maintenance of records, audit of policies, data protection officer, processing by entities other than fiduciaries, grievance reversal by data fiduciary. Again some of these things you will remember we have covered in some aspects earlier in the fair information practices week.

(Refer Slide Time: 3:11)



So, one of the critical things that this bill is actually proposing is to set up a Data Protection Authority of India. So Data Protection Authority of India, the role, what it should do, what is the mandate for it, who will be the body which is part of this authority, what all can they do or what all they cannot do, all of that is listed in some versions here, so which is the establishments of the authority, composition and qualifications, terms and conditions of appointment, removal of chairpersons, power of chairpersons. Meetings of authority, vacancies, offices, code of practices, all that, so they went in slightly detail of how to set up the authority itself, which is discussed here.

(Refer Slide Time: 4:05)

**THE PERSONAL DATA PROTECTION BILL, 2019**

A  
BILL

*to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organizational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorized and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.*

**WHEREAS** the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy,

**AND WHEREAS** the growth of the digital economy has expanded the use of data as a critical means of communication between persons;

NPTEL  
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY  
HYDRABAD

So, now let us look at in detail some aspects of this bill. Again I will highly, highly recommend you to read it yourself fully and if there is any discussion that you want to have it with me I will be happy to speak with you, and not just with you, for the entire class also. So let us read what is this Act or bill, what is this bill all about?

The Personal Data Protection Bill is to provide for protection of privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities, processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organizational and technical measures and processing of data.

Laying down norms for social media intermediary, cross-border transfer, accountability of entities, processing personal data, remedies for unauthorized and harmful processing and to establish Data Protection Authority of India for the purpose, for the said purpose and for matters connected therewith or incidental thereto. All right.

So that is what the bill is all about, explaining details about what information could be collected, who can have access to it, what situation the information could be collected about the authority itself, whereas the right of privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy and whereas the growth of a digital economy has expanded the use of data as a critical means of communication between persons.

So we will actually come back to this how data is becoming a more and more important thing even from the Non-personal Data Protection Framework that we will discuss also, where data is basically the way that companies and organizations are talking about right now. So that is what the PDP Bill is, so that gives you a sense of what the bill is all about. So, let us go over the bill section by section and see what all components the bill has, what are the protection that it gives, what features does it have all that in detail.

(Refer Slide Time: 6:35)

NPTEL

digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto.

Be it enacted by Parliament in the Seventeenth Year of the Republic of India as follows:—

CHAPTER I  
PRELIMINARY

1. (1) This Act may be called the Personal Data Protection Act, 2019.  
(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

2. The provisions of this Act,—  
(A) shall apply to—  
(a) the processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India;  
(b) the processing of personal data by the State, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law;  
(c) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is—

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY  
HYDRABAD

I have highlighted the parts that we will actually look into detail. I will also share this annotated document as in the slides before, so you will get access to what all annotations that have done also.

(Refer Slide Time: 6:49)

The slide contains the following definitions:

- (10) "consent" means the consent referred to in section 11;
- (11) "data" includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;
- (12) "data auditor" means an independent data auditor referred to in section 29;
- (13) "data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;
- (14) "data principal" means the natural person to whom the personal data relates;
- (15) "data processor" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary;
- (16) "de-identification" means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;
- (17) "disaster" shall have the same meaning as assigned to it in clause (d) of section 2 of the Disaster Management Act, 2005;
- (18) "financial data" means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history;

So who is the data fiduciary? The word data fiduciary comes up so many times in this PDP Bill, so we need to know what the definition of the data fiduciary is. Data fiduciary means any person including the state, a company, a juristic entity or any individual who alone or in conjunction with others determines the purpose and the means of processing of the personal data. So who is deciding on what the data should be processed for that is data fiduciary.

All right, so I am going slowly, so you will get a sense. This document links are also on the slides, so you should be able to get to that, you can go through the document yourself but some parts I will actually enable a discussion around it.

(Refer Slide Time: 7:48)

The slide contains the following provisions:

6. The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.

7. (1) Every data fiduciary shall give to the data principal a notice, at the time of collection of the personal data, of all the data to be collected from the data principal, in so far as reasonably practicable, containing the following information, namely:—

- (a) the purposes for which the personal data is to be processed;
- (b) the nature and categories of personal data being collected;
- (c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable;
- (d) the right of the data principal to withdraw his consent, and the procedure for each withdrawal, if the personal data is intended to be processed on the basis of consent;
- (e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds specified in sections 12 to 14;
- (f) the source of such collection, if the personal data is not collected from the data principal;
- (g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;
- (h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;
- (i) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;
- (j) the existence of and procedure for the exercise of rights mentioned in Chapter V

processing of personal data

(a) the purposes for which the personal data is to be processed;

(b) the nature and categories of personal data being collected;

(c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable;

(d) the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;

(e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds specified in sections 12 to 14;

(f) the source of such collection, if the personal data is not collected from the data principal;

(g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;

(h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;

(i) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;

(j) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same;

(k) the procedure for grievance redressal under section 32;


(l) the existence of a right to file complaints to the Authority;

(m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and

(n) any other information as may be specified by the regulations.

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY  
HYDERABAD



processing of personal data

(f) the source of such collection, if the personal data is not collected from the data principal;

(g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;

(h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;

(i) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;

(j) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same;

(k) the procedure for grievance redressal under section 32;


(l) the existence of a right to file complaints to the Authority;

(m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and

(n) any other information as may be specified by the regulations.

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY  
HYDERABAD



So this one is the fundamental thing that we have seen right notice, so every data fiduciary shall give to the data principle a notice, data principle is the owner of the data principle notice, at the time of the collection of the personal data or if the data is not collected for the person from the data principle as soon as reasonably practicable containing the following information namely.

So it could be the case that Amazon is collecting data from me, I know that Amazon is collecting data, it could be the case that I do not even know Amazon is going to get access to this data. So that is what they are saying and if the data is not collected from the data principle, if it is not directly collected from me as soon as I get in touch with the data being collected, I should be notified that.

The purpose for which their personal data is being processed, the nature and categories of personal data being collected, so I think some of this is repeating. I consciously have left it the way it is, it is repeating because I think you will get to know the importance of some of these topics as you see it in multiple places, where information practices we saw, privacy policies we saw, now we are seeing in GDPR or in PDP Bill.

And then you will see it in GDPR. The nature and categories of personal data being collected, the identity and contact details of the data fiduciary and contact details of the data protection officer if applicable, the right of the data principle to withdraw his consent and procedure for such withdrawal, if the personal data is intended to be processed on the basis of the consent. I mean, I should have the right to say that, look you cannot collect my data.

I should have the right to be forgotten, erased, all that will come later, but that is the theme here and the end user, the customer should have the right. The bases for such pre-process, such processing and the consequences of failure to provide such personal data if processing of the personal data is based on the grounds specified in section 12 to 14, the source of such collection if the personal data is not collected from that data principle.

I mean, if they are collecting some information about me from a different source that source also should be notified for me. Individual entities including other data fiduciaries or data processors, with whom such personal data may be shared if applicable. Amazon is collecting data from us for delivering a book, but amazon is also sharing that detail to a courier company or a delivery company, who knows the data, who has my cell number to come and deliver the book, that is what the third party could be here.

Information regarding any cross-border transfer of personal data that the data fit usually intends to carry out which is data from India being collected is going, for an Indian citizen is collected and it is being moved to the US, stored there or a data being collected in India for Europe Company, Europeans, data is being collected in Europe and then transferred in the US, all of this is cross-border policies, so that has to be explicitly stated.

The period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period. So this period generally is mentioned as how long the data will be kept. The existence of and procedure for exercise of rights mentioned in chapter five, the procedure for grievance, so all of this is slightly more in detail, but for us the important things were the first few which is data being collected, cross-



border, who has access to the data, what all information should be provided to the user before the data is being collected, all that. Hope that gives you a sense.

(Refer Slide Time: 12:21)

Interpreting in a dominant person into its native language where necessary and practicable.

(3) The provisions of sub-section (1) shall not apply where such notice substantially prejudices the purpose of processing of personal data under section 12.

**K (1)** The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed. *Quality of personal data processed.*

(2) While taking any steps under sub-section (1), the data fiduciary shall have regard to whether the personal data—

- (a) is likely to be used to make a decision about the data principal;
- (b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or
- (c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.

(3) Where personal data is disclosed to any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirement of sub-section (1), the data fiduciary shall take reasonable steps to notify such individual or entity of this fact.

**9.(1)** The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing. *Restriction on retention of personal data.*

(2) Notwithstanding anything contained in sub-section (1), the personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to

Again this is the PDP Bill, so which is under which is under review, so once this comes through hopefully it will be an act and you all can actually benefit from the advantages that the PDP Bill is providing us which is more and more privacy aware policies being created for the data that is collected in India. Especially about the Indian citizens also. The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated having regard to the purpose for which it is processed.

My information should be collected and it should be accurate, they cannot take my information as male and change it as female, profile picture or a passport graph, photograph that is taken from me and then instead of me there is somebody else in my Government records, I think these cannot happen.

(Refer Slide Time: 13:39)

(4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations.

10. The data fiduciary shall be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf.

Accountability of data fiduciary.

11. (1) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.

Consent necessary for processing of personal data.

30 (2) The consent of the data principal shall not be valid, unless such consent is—

1872 (a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;

35 (b) informed, having regard to whether the data principal has been provided with the information required under section 7;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

40 (e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

The date of fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at end of the processing. The data, Amazon takes the data for submission of delivery of the goods and they have let us take a 30 day or a 10 day return policy, the return policy time is also done, now why does amazon need to store my details.

So that is the kind of point here, that the fiduciary should be, fiduciary should delete the details after the transactions is done and the due diligence for, and the due time is given for anything around the transaction. The date of fiduciary shall be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf.

On its behalf is also important, if amazon is letting a third party to do the transactions that third party also should be protected, should give us protection for the data that is being collected from us. The personal data shall not be processed, except on the consent given by the data principle at the commencement of its processing. Only for the data that I have given consent the processing should be done. They cannot just collect all data and then process all of them.

(Refer Slide Time: 15:25)

(j) Where the Authority specifies a reasonable purpose under sub-section (i), it shall—

(a) lay down, by regulations, such safeguards as may be appropriate to ensure the protection of the rights of data principals; and

(b) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.

40

15. (1) The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data", having regard to—

45

Category of personal data as sensitive personal data.

(a) the risk of significant harm that may be caused to the data principal by the processing of such category of personal data;

(b) the expectation of confidentiality attached to such category of personal data;

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDRABAD

So, there is also this provision of Central Government organizations have a different way of looking at this data provisions being given for them. The Central Government shall, in consultation with authority and the sectoral regulator concerned, notify such categories of personal data, sensitive personal data having regard to the risk of significant harm, the expectations of confidentiality attached whether significantly discernible class of data principles may suffer the adequacy of protection afforded by ordinary provisions applicable to personal data.

So essentially what this is saying that the Central Government or the government will have a way by which it will classify the personal data and give a list of what is personally identifiable, what is sensitive, what is super sensitive, all that. I think, this list is an important list to have and every country has been producing such kind of a list, which keeps changing over a period of time also, so having such a list is very important.

(Refer Slide Time: 16:45)

The slide contains text from a legal document, likely the Indian Data Protection Bill. It includes the NPTEL logo on the left and the International Institute of Information Technology Hyderabad logo on the right. The text discusses the right to correction and erasure of personal data. A yellow scribble is present over the text. A video inset in the bottom right shows a man with a beard and glasses wearing a yellow shirt.

provided in the notice under section 7 in relation to such processing.

(2) The data fiduciary shall provide the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person.

(3) The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.

10 **18. (1)** The data principal shall, where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to— Right to correction and erasure.

15 (a) the correction of inaccurate or misleading personal data;

(b) the completion of incomplete personal data;

(c) the updating of personal data that is out-of-date; and

(d) the erasure of personal data which is no longer necessary for the purpose for which it was processed.

(2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with such correction, completion, update or erasure having regard to the purposes of processing, such data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application.

20 (3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal.

25

The data principle shall where necessary having regard to the purposes for which the personal data is being processed, subject to such conditions and in such manner as may be specified by regulations have the right to - correction of inaccurate information, completion of incomplete, updation of personal data that is out of date and erasure of personal data which is no longer necessary for the purpose of which it was processed. As user you should have access to changing the data, asking the company to delete all that.

(Refer Slide Time: 17:26)

The slide continues the text from the previous slide, discussing the right to data portability. A yellow scribble is present over the text. A red circle with the word 'JSON' is drawn around the text. A video inset in the bottom right shows the same man in a yellow shirt.

by the data principal.

(4) Where the data fiduciary corrects, completes, updates or erases any personal data in accordance with sub-section (1), such data fiduciary shall also take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, update or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them.

30 **19. (1)** Where the processing has been carried out through automated means, the data principal shall have the right to— Right to data portability.

35 (a) receive the following personal data in a structured, commonly used and machine-readable format—

(i) the personal data provided to the data fiduciary;

(ii) the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or

(iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and

40 (b) have the personal data referred to in clause (a) transferred to any other data fiduciary in the format referred to in that clause.

(2) The provisions of sub-section (1) shall not apply where—

(a) processing is necessary for functions of the State or in compliance of law or order of a court under section 12;

45 (b) compliance with the request in sub-section (1) would reveal a trade secret of any data fiduciary or would not be technically feasible.

Where the processing has been carried out through automated means, the data principle shall have the right to receive the following personal data in a structured commonly used and a

machine-readable format. So in these days probably this is going to be in JSON. All right. So, what this is? This this provision is for you to go ask Facebook saying please give me all the data that you have about me and this is these features are already there because I think in the US and in Europe these have become very required.

GDPR also makes it mandatory, so therefore, there is a provision of you asking for information what the companies have about you and clicking few buttons and getting that as a JSON object, but we will also have to keep in mind what they are sharing and what they are not sharing, in the file that they are giving you, are they sharing everything that they know, I think, some evaluations have to be done there.

The personal data provided to the data fiduciary, at least, here they are saying that what is that they have, personal data provided to the data fiduciary, the data which has been generated in the course of provisions of services, use of data, use of goods by the data fiduciary or the data which forms part of any profile of a data principle. Because I think the companies when they collect data the data itself is important, of course.

But the inferences that they make out of the data is much more important for them. Their choices that they are going to make is going to be dependent on the data that they have and the inferences that they are drawing on it. Keeping that in mind I think, if we get access to, if the companies have access to the inferences and we are able to know from where the companies made their inferences through this way by which we can ask data, what they have, I think it will be super nice.

(Refer Slide Time: 19:49)

where such compliance shall harm the rights of any other data principal under this Act.

NPTEL

CHAPTER VI  
TRANSPARENCY AND ACCOUNTABILITY MEASURES

22. (1) Every data fiduciary shall prepare a privacy by design policy, containing—

(a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;

(b) the obligations of data fiduciaries;

(c) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;

(d) the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;

(e) the protection of privacy throughout processing from the point of collection to deletion of personal data;

(f) the processing of personal data in a transparent manner; and

(g) the interest of the data principal is accounted for at every stage of processing of personal data.

(2) Subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy prepared under sub-section (1) to the Authority for certification within such period and in such manner as may be specified by regulations.

(3) The Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1).

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY  
HYDRABAD

Privacy by design policy.

So every data fiduciary shall prepare a privacy by design policy containing the managerial organizational business practices and technical systems, obligations of data fiduciary, the technology used in the processing, the legitimate interest of business including any innovation is achieved, the protection of privacy, the processing of personal data.

The interest of data principle is accounted for every stage, for at every stage of processing of personal data, so these things are details, but I think these are very, very relevant for having the protection of the personal data that is collected from the principle. And this privacy by design privacy policies are one way by which companies can actually express what they are doing, which we have seen in detail earlier part of this course.

(Refer Slide Time: 20:52)

which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform.

24. (1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including—

- (a) use of methods such as de-identification and encryption;
- (b) steps necessary to protect the integrity of personal data; and
- (c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.

25. (1) Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.

(2) The notice referred to in sub-section (1) shall include the following particulars, namely—

- (a) nature of personal data which is the subject-matter of the breach;
- (b) number of data principals affected by the breach;
- (c) possible consequences of the breach; and
- (d) action being taken by the data fiduciary to remedy the breach.

Every data fiduciary that shall take necessary steps to maintain transparency in processing personal data and shall make the following information available in such form and manner as may be specified by regulations. The categories of personal data are generally collected in the manner of such collection. The purpose for which the personal data is being generally processed, so this word transparency also is becoming more and more important.

Fairness, accountability and transparency, these are called fact, fairness, accountability and transparency, I mean Amazon making some choices with the data and inferences from the data that they collected from us can they let everybody know how they are making the choices, how they are making the recommendations. Being transparent makes it very equitable for everybody but again a company's advantage, business advantage also may be the reason why the transparency is much harder for the companies.

Every data fiduciary and data processor shall having regard to the nature scope and purpose of processing personal, there risks associated with such processing and the likelihood and severity of their harm that may result from such processing implement necessary security guards including, so this is more the security safeguards. So, it says de-identification encryption, integrity of the personal data, so all of this we have seen in the past.

(Refer Slide Time: 22:51)

25. (1) Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.

(2) The notice referred to in sub-section (1) shall include the following particulars, namely—

- (a) nature of personal data which is the subject-matter of the breach;
- (b) number of data principals affected by the breach;
- (c) possible consequences of the breach; and
- (d) action being taken by the data fiduciary to remedy the breach.

(3) The notice referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and within such period as may be specified by regulations, following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm.

(4) Where it is not possible to provide all the information specified in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay.

(5) Upon receipt of a notice, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.

Every data fiduciary shall by notice so and the other thing that I am kind of hoping that you will you will connect the dots is that we have seen many concepts in the class and it is all coming together in this PDP Bill. You will see that it is connected in GDPR also and, so all of these concepts are coming together, which also makes it more interesting that you are aware, if you read these policies, if you read these Acts and bills yourself, you should be able to connect almost everything that is discussed in this document.

Every data fiduciary shall by notice inform authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principle. So this is also an important one which is the, if my data is breached, if you are running a company and if you have my data and the data got breached, the server got hacked or you stole or you misplaced the data and this data was lost, in all of these scenarios I should be notified that such a breach has happened.

And in the past I have been, my data has been part of some of these breaches and I have got physical letters email saying that your, there is a possibility that your data is in, is part of this data leak, so please go ahead and change the password please, come to our bank and change the physical card all that, that is what is mentioned here, which is it is necessary for the companies to actually make this accountable, make the company accountable by saying that you should do this.



(Refer Slide Time: 24:43)

(5) On receipt of the assessment and its review, if the Authority has reason to believe that the processing is likely to cause harm to the data principals, the Authority may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as the Authority may deem fit.

28. (1) The significant data fiduciary shall maintain accurate and up-to-date records of the following, in such form and manner as may be specified by regulations, namely:—

- (a) important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 10;
- (b) periodic review of security safeguards under section 24;
- (c) data protection impact assessments under section 27; and
- (d) any other aspect of processing as may be specified by regulations.

(2) Notwithstanding anything contained in this Act, this section shall also apply to the State.

(3) Every social media intermediary which is notified as a significant data fiduciary under sub-section (4) of section 26 shall enable the users who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed.

(4) Any user who voluntarily verifies his account shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.

29. (1) The significant data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this

The significant data fiduciary shall maintain accurate and up-to-date records of the following in such form and manner as may be specified by regulations namely important operations in the data life cycle, a periodic review of the security safeguards, data protection impact assessment and any other aspect of processing as may be specified by the regulations. So the company also should have a track of all the measurements that the company has taken, data fiduciary has taken to protect the data.

(Refer Slide Time: 25:19)

form of a data trust score having regard to the factors mentioned in sub-section (2).

(7) Notwithstanding anything contained in sub-section (1), where the Authority is of the view that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal, the Authority may direct the data fiduciary to conduct an audit and shall appoint a data auditor for that purpose.

30. (1) Every significant data fiduciary shall appoint a data protection officer possessing such qualification and experience as may be specified by regulations for carrying out the following functions—

- (a) providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act;
- (b) monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act;
- (c) providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review under sub-section (4) of section 27;
- (d) providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22;
- (e) providing assistance to and co-operating with the Authority on matters of compliance of the data fiduciary with the provisions under this Act;
- (f) act as the point of contact for the data principal for the purpose of grievances redressal under section 32; and
- (g) maintaining an inventory of records to be maintained by the data fiduciary under section 28.

So continuing in the, looking at the different parts of PDP Bill, here is the next one data protection officer. Every significant data fiduciary shall appoint data protection officer

possessing such qualification and experience as may be specified by regulations for carrying out the following functions. So, I think, this chief privacy officer, chief data protection officer, all of these are roles that have been generated created because of these kind of regulations now.

I do not think so 15 years before, 20 years before there was anything called as chief privacy officer, today if you see chief privacy officer has become very common in companies, so therefore, the proposal here is to have data protection officer, which may be slightly different from the privacy officer.

(Refer Slide Time: 26:13)

(3) Any transfer under clause (a) of sub-section (2) shall be notified to the Authority within such period as may be specified by regulations.

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

CHAPTER VIII  
Exemptions

20 35. Where the Central Government is satisfied that it is necessary or expedient,—

Power of Central Government to exempt any agency of Government from application of Act.

(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or

(ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order,

25 it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.

30 Explanation.—For the purposes of this section,—

(i) the term "cognizable offence" means the offence as defined in clause (c) of section 2 of the Code of Criminal Procedure, 1973;

So this is the exemptions for Central Government where the Central Government is satisfied that it is necessary or expedient in the interest of sovereignty and integrity, sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order or for preventing incitement to the commission of any cognizable offense relating to sovereignty and integrity of India.

So, essentially what this means is that Central Government has access to, can be exempted from collecting information, exempted from providing protection to the data for national level problems, that is what this part is trying to say. Giving the government a way by which they do not have to, for example, like case is getting investigated, they do not have to actually get worried about or protection, concerned, all of this, that is the protection that... But it is an exemption but this exception comes from, with lot of processes that has to be taken care of.

(Refer Slide Time: 27:36)

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY  
HYDRABAD

(b) the purpose of collection of personal data for disclosure to any other individuals or entities; and

(c) the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.

40. (1) The Authority shall, for the purposes of encouraging innovation in artificial intelligence, machine learning or any other emerging technology in public interest, create a Sandbox.

21

(2) Any data fiduciary whose privacy by design policy is certified by the Authority under sub-section (3) of section 22 shall be eligible to apply, in such manner as may be

So next one is a very computer sciencey thing, which is the authority shall for purposes of encouraging innovation and artificial intelligence, machine learning or any other emerging technology in public interest create a sandbox. So the sandbox is, I think, many implementation these days have sand boxes, the idea is that they create a sandbox where you can actually go apply your algorithms to check.

Let us take if they have data, you can put in your algorithm to check what the results for the data are, some of the sandboxes that we have done is in the healthcare sector where they have created a sandbox, they have created a place where we can actually set up our code and interact with the data that they have kept through APIs to see how decisions could be made, how our implementation can be improved and all that.

Sandpit where the kids play, that is the analogy here, I mean, in any place you can put a small space for sand pit where kids can play, they will not get hurt and everything that is the idea for sandbox here and you will not have access to the entire data that, entire data or entire infrastructure the company or the organization has also. Restricted view of what the company does is the sandbox.

(Refer Slide Time: 29:11)

(iv) the restriction on retention of personal data under section 9.

**CHAPTER IX**  
**DATA PROTECTION AUTHORITY OF INDIA**

34 41. (1) The Central Government shall, by notification, establish, for the purposes of this Act, an Authority to be called the Data Protection Authority of India. Establishment of Authority.

(2) The Authority referred to in sub-section (1) shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.

35 (3) The head office of the Authority shall be at such place as may be prescribed.




(4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.

42. (1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be a person having qualification and experience in law. Composition and qualifications for appointment of Members.

(2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of—

(a) the Cabinet Secretary, who shall be Chairperson of the selection committee;

45 (b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and



Central Government shall by notification established for the purposes of this Act and authority to be called as Data Protection Authority of India. So, if this bill gets passed there will be a organization called Data Protection Authority of India and the rest of this PDP Bill goes into details of what this authority should be, who should be recruited, who should be on the board, what all powers do they have, all that, I do not think so that is that much required for the class so I am going to skip all of that.

But the rest of the document is only about Authority of India, so I do not think so there is anything highlighted after this, let me make sure that I am not missing anything. Yeah, after this the end of the document just summarizes all the clauses that are mentioned in the document. So, that is the PDP Bill.

(Refer Slide Time: 30:22)

The screenshot shows the first page of the regulation document. At the top left is the NPTEL logo with the text 'NPTEL A S 2016'. At the top center is the text 'Official Journal of the European Union'. At the top right is the logo of the International Institute of Information Technology Hyderabad. The page is numbered '1' and is titled 'Legislative acts'. The main heading is 'REGULATIONS'. The title of the regulation is 'REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)'. It includes the text '(See with EEA relevance)', 'THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION', and 'Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof, Having regard to the proposal from the European Commission.'

The screenshot shows the second page of the regulation document. It continues with 'Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof, Having regard to the proposal from the European Commission, After transmission of the draft legislative act to the national parliaments, Having regard to the opinion of the European Economic and Social Committee (5), Having regard to the opinion of the Committee of the Regions (5), Acting in accordance with the ordinary legislative procedure (5), Whereas: (1) The protection of natural persons in relation to the processing of personal data is a fundamental right.'

Now let us look at GDPR. So, what all we have done? We have already done looking at the IT Act 2000 the amendments and the PDP Bill. Now, let us go outside India to look at what GDPR is and then we will come back and look at the NPD - Non-personal Data Framework. This GDPR document will look very similar to the PDP Bill. Probably PDP got inspired by the committee that wrote the PDP Bill, got very much inspired by GDPR.

And therefore, they kind of took a lot of inspiration from here, so I am going to highlight some of it, and for redundancy purposes also I have kept some parts to be repeating from what we have already seen to make sure that you understand the importance that it is covered in GDPR and PDP Bill also.

Initially there is a lot of introduction for the problem, context, scenario, setting, all that is happening in the document and they talk about articles, so we will jump directly to the different articles that are there in the document.

(Refer Slide Time: 31:43)



The slide displays the following definitions for the purposes of the Regulation:

- (1) **personal data** means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (3) **restriction of processing** means the marking of stored personal data with the aim of limiting their processing in the future;
- (4) **profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement;
- (5) **pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- (6) **storage limitation** means any restriction set of personal data which are accessible according to specific criteria, whether controlled, determined or disposed on a functional or geographical basis;
- (7) **controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

So from here is what the articles of the GDPR comes, so we will go through some again important ones, rest I will leave it for you to digest it to yourself. So the definitions, again you should look at these kind of documents to give some clarity on the definitions that we have seen in the class until now also. So this says, personal data means any information relating to an identified or identifiable natural person that is data subject.

An identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier such as a name, an identification number, location, an online identifier or to one or more factors specific to the physiological, genetic, mental, economic, cultural or social identity of the natural person. What an interesting way of defining about a person, details that they have provided. Any information about you and me will fall their personal data that can be identified.

Processing means any operation or set of operations which is performed on personal data, on sets of personal data whether or not by automated means such as collecting, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or, combination, restrictions, erasure or destruction. Any of this if you do with the data that is called processing. Very detailed, very intense in that sense also.

(Refer Slide Time: 33:49)

 **controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) **processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the

---

1974  Official Journal of the European Union 4.5.2

framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipient; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

(10) **third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised



 **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the

---

974  Official Journal of the European Union 4.5.201


framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipient; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

(10) **third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) **consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;



 **consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;


(13) **genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) **biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) **'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) **'main establishment'** means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;



Let us jump to controller, again there are many other definitions, I am connecting to only some things that we have seen in the class. Controller means the natural or the legal person, public authority, agency or other body, which alone or jointly with others determines the purposes and means of the processing of personal data, where the purposes and the means which is processing or determine by Union or Member State Law.

The controller or the specific criteria for its nomination may be provided by the union or the member state law. So this is basically person who has control over the data, it can be the state, it can be state representatives it can be an organization. Processor means a natural or a legal person, public authority or an agency or other body which processes personal data on behalf of the controller.

It could be, this processor could be Amazon for that matter. Recipient means a natural or a legal person, public authority, agency or another body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State Law shall not be regarded as recipients.

Recipients is a body with personal data or disclosure meaning, who is getting the data. Third party means a natural or a legal person, public authority, agency or a body, other than the data subject, controller, processor and persons who, under third party could be the delivery person that I mentioned earlier about Amazon.

Consent of the body, of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her. I bought a book on Amazon, I am giving the concern for amazon to use the data to personalize my search results in future.

Personal data breach which means breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. Somebody hacking into LinkedIn data server that is the personal data breach. So please feel free to take a look at this document again.

Whichever parts you are interested in, there is a lot of interesting ramifications of this GDPR and PDP Bill that people are thinking about, worried about sometimes because I think it is



very hard to, I think, it is very hard to implement all of this very well and do well in business also. And another way of saying is that companies are going to have a lot more work in terms of giving all these protection, giving all these disclosures and making sure that all the policies are maintained and still do their business well.

(Refer Slide Time: 37:39)

The slide displays the following text:

**Article 10**  
**Processing of personal data relating to criminal convictions and offences**  
Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

**Article 11**  
**Processing which does not require identification**

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER 01

Article processing of personal data relating to criminal convictions and offenses, processing of personal data relating to criminal convictions and offenses or related security measures based on Article 6(1), shall be carried out only under the control of the official authority or when the processing is authorized by the Union or Member State Law providing for appropriate safeguards for the rights and freedoms of data subjects. So, this is basically if anybody is getting access to criminals, data, it can be given only under a certain level of protection and only authority level X and above will get access to that data.

(Refer Slide Time: 38:24)

Official Journal of the European Union L 11943

Article 15

**Right of access by the data subject**

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall

The right of access by data subject, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and where that is the case, access to the personal data and following information, the purpose of the processing, the same list, the purpose of the processing, categories of personal data concerned all of that should be available for the subject to know that the company is doing with my data.

(Refer Slide Time: 38:55)

Official Journal of the European Union L 11944

Article 17

**Right to erasure (right to be forgotten)**

1. The data subject shall have the right to obtain from the controller without undue delay the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

Right to rectification there are data subjects, I will have the right to obtain from the controller without undue delay, important thing, without undue delay the rectification of inaccurate

personal data concerning him or her. Taking into account the purpose of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing supplementary statement.

So this unduly, undue delay I mentioned because you can ask the company for the data and the company can take like as long as they want to give you the data is not possible. It has to be given in certain timeframe. Right to erasure - The data subject shall have the right to obtain from the controller, the erasure of personal data concerning him or her, without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies. My information, I should have the right to raise.

(Refer Slide Time: 40:01)

The screenshot shows a presentation slide with the following content:

- Right to data portability**
- 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
  - the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
  - the processing is carried out by automated means.
- 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
- 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4  
**Right to object and automated individual decision-making**  
Article 21  
**Right to object**

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, of one of the following:

The slide also features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. A video inset in the bottom right corner shows a man with a beard and glasses speaking.

Right to data portability - The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller in a structured commonly used and machine readable format. So this is again portability that we saw in PDP Bill also where I can go to Amazon and say please give all the data that you have about me, particularly they should give it in a machine readable format, which I mentioned earlier could be JSON.

(Refer Slide Time: 40:35)

**Automated individual decision-making, including profiling**

**NPTEL** The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.


2. Paragraph 1 shall not apply if the decision:

- (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- (c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 3  
**Restrictions**  
Article 23



The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. So this is shall have the right not to be subject to decision based, so Amazon should not be just making decisions only by automated methods on the things that they are doing with my data.

(Refer Slide Time: 41:14)

**Notification of a personal data breach to the supervisory authority**

**NPTEL** The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

**Notification of a personal data breach to the supervisory authority**


1. In the case of a personal data breach, the controller shall, without undue delay and, where feasible, not later than 72 hours after becoming aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 30, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;
- (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where used in this Article, it is understood that the notification to the supervisory authority shall include information on:



More details about the GDPR, notification of a personal data breach to the supervisory authority. In the case of, take a look at the time and everything, details that they have provided here. In the case of personal data breach which we also saw in PDP Bill, the

controller shall without undue delay and where feasible not later than 72 hours after having become aware of it notify the personal breach to the supervisory authority competent in accordance with the article 55.

Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the natural persons. Where the notification to the supervisor authority is not made within 72 hours it shall be accompanied by reasons for the delay, so I think GDPR is going a little one step ahead, not just saying that, oh, it should be notified, it should be notified within 72 hours, is the argument that the GDPR is making.

And if it is not made within 72 hours explanation has to be given, so again rest a lot of details about what all could be done, what all cannot be done, authority, all the details is there in the rest of the GDPR document. I will let you again, it is an 88 page document, I will let you to go through it yourself if it is of interest to you. So that gives us a sense of what is going on in the world. These are these are the important ones, GDPR is a prominent one. PDP Bill in India is an extremely important one where the world is looking at when we will have some kind of a conclusion and acceptance of the bill that is being presented.

(Refer Slide Time: 43:07)



The slide features the NPTEL logo on the top left and the IIIT Hyderabad logo on the top right. The main text is centered and reads: "Report by the Committee of Experts on Non-Personal Data Governance Framework". In the bottom right corner, there is a small inset video of a man with a beard and glasses, wearing a yellow shirt, with his hands clasped in front of him.



## Experts on Non-Personal Data Governance Framework



U1 - X-Y - A  
U2 - Z - G - B



Now, let us look at the NPD. I think my goal for having the NPD part is from the point of view of comparing it with the personal data because it is not a lot of details that I want to go through in the NPD as part of this class. So we looked at personal data, personal data is your cell number, my cell number all that. Non-personal data also can be actually used very well for making decisions, very much useful in improving the society all that can happen with the non-personal data also.

What is a non-personal data? Non-personal data you could think of it as if, meaning, I am taking Uber from IIIT Hyderabad to airport, I am, PK taking the Uber and I am on the cab going from here to airport could be probably personal data, but if you just think about it, if Uber could be asked a question that look give us the number of people who are on the road from IIIT to Hyderabad to airport that number that aggregate information may not be personal.

Does not have to be just only that level, it could be, give us the age bracket between 20 to 40 or 40 to 80 or something like that, so if such kind of details which is, if you remember we also talked about in anonymization techniques, so if Uber was to give, saying here is the user 1 age group X to Y is on route to airport, user 2 Z to A, Z to G, age group and is on the route 2 airport at a point of B.

This level of information can be extremely useful for many things, for example, you could think of using this information for designing the signal, a traffic signal system, based on the number of cars that could be around that location. Uber data can be extrapolated and used to make this choice. There are many such information, meteorological information, climatic

details about a location can be used for social good if it was being used and if it was being corroborated with the other information that is available which could be personal information.

So that is the idea, non-personal data is a set of data that is available, not identifiable to individuals, but still being very useful for making decisions, how can you now do business, how can you now make empower organizations, empower citizens with this non-personal data, so something socially good can be done and something, world can be a little bit a better place to live, that is the goal here.

(Refer Slide Time: 46:47)

NPTEL 1972/2020/CL&ES 272 INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDRABAD

Contents

1. Brief of the Committee	3
2. Methodology	3
3. Data – Trends and Socio-Economic Impact	5
4. Definition of Non-Personal Data and Key Roles	13
5. Ownership of data	23
6. Undertaking a Data Business	27
7. Data Sharing	32
8. Non-Personal Data Regulatory Authority	40
9. Technology Architecture	44
10. Summary	46
Appendix 1: List of Committee Members	54
Appendix 2: Examples of Non-Personal Data	55
	--



NPTEL COMMITTEE DISCUSSIONS AND RECOMMENDATIONS INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDRABAD


### 3. Data – Trends and Socio-Economic Impact

**Key Take-Aways**

- The world is awash with data.
- The proliferation of big data, analytics and Artificial Intelligence (AI) has led to the creation of many new information intensive services and also the transformation of existing businesses.
- Data inter alia contributes to economic value and wealth. Frameworks are being created to better understand the uses and benefits of data.
- Organizations have been discovering ways to generate value from data. The digital economy is witnessing the emergence of a few dominant players and a certain imbalance in the market.
- Given the increasing importance and value generation capacity of the data economy, governments around the world realise the need to enable and regulate all aspects of data, both Personal and Non-Personal Data.

**Data availability and value generation from data**

3.1. The world is awash with data. Planet scale adoption of the internet, smartphones, and cloud storage, has led to generation of AI systems on the scale



Again I will let you to go through this, I mean, at least, I was very happy to be part of this committee to do the deliberations and everything.

(Refer Slide Time: 47:06)

The slide contains the following text:

**4.7. Data Principal**

- i. In case of Personal Data, data principal is the natural person to whom the personal data relates. However, in case of Non-Personal Data, the definition of a data principal is related to the type of Non-Personal Data - Public, Community and Private data, as well as based on different possible kinds of subjects of data.
- ii. In case of Public Non-Personal Data:
  - o Government may collect data pertaining to citizens (like census), companies (like company registration, financial filings) and communities.
  - o The data principal will be the corresponding entities (individuals, companies, communities) to whom the data relates.
- iii. In case of Private Non-personal Data:
  - o Private sector may collect data pertaining to citizens (like customer surveys), companies (like vendor registration, vendor product information) and communities.
  - o The data principal will be the corresponding entities (individuals, companies, communities) to whom the data relates.

The slide also features the NPTEL logo, the number 1972, and the logo of the International Institute of Information Technology (IIIT) Hyderabad. A video inset shows a man with a beard and glasses, wearing a yellow shirt, speaking.

So again I will let you go through it but earlier in this week I said there is this whole thing of data with which amazing things could be done, non-personal data is one piece, we do not generally talk about it. We have always spoken about a personal data only. Yeah, please go through this document. My intent here was to compare it with the personal data and to highlight the point that the non-personal data also should be protected in one sense and should be available for making business values.

(Refer Slide Time: 47:43)

The slide displays the title page of the Information Technology Act, 2000. The text on the page includes:

**IT Act 2000**

चक्र 27] सं संसदीय, सुक्रमा, सुक्र 8, 2000 / संसद 19, 1922  
No. 27] NEW DELHI, FRIDAY, JUNE 3, 2000 / JYAISTHA 13, 1922

इस भाग में दिए हुए संख्या दी जाती है जिससे कि यह आलाय कबलाय के रूप में लुका जा सके।  
Separate paging is given to this Part in order that it may be filed as a separate compilation.

**MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department)**

New Delhi, the 9th June, 2000/Jyaisika 19, 1922 (Saka)  
The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:—

**THE INFORMATION TECHNOLOGY ACT, 2000**  
(No. 21 of 2000)

[19th June, 2000]  
An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate

The slide also features the NPTEL logo, the number 1972, and the logo of the International Institute of Information Technology (IIIT) Hyderabad. A video inset shows the same man from the previous slide speaking.





**MINISTRY OF LAW AND JUSTICE**  
(Legislative Department)

New Delhi, the 5th February, 2008 (Single 11, 1999 (Date)

The following Act of Parliament received the assent of the President on the 5th February, 2008, and is hereby published for general information—

**THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008**  
No. 13 of 2008 [14 February 2008]

An Act further to amend the Information Technology Act, 2008.

Enacted by Parliament in the Fifty-eighth Year of the Republic of India as follows—

**PART I**

**A. Preamble:**

1. (1) This Act may be called the Information Technology (Amendment) Act, 2008.

(2) It shall come into force on such date as the Central Government may, by notification

## IT Act 2008 Amendment



**REGULATIONS**

**REGULATIONS AND ORDER OF THE INFORMATION TECHNOLOGY AND OF THE CERTIFICATES**  
17 April 2008

on the provisions of certain provisions with respect to the processing of personal data and on the fee structure of such data, and regarding Director (IT) and Director (Data Protection) Regulations

On such date as the

The Information Technology and of the Certificates

Being signed by the Director of the Information Technology and of the Certificates

Being signed by the Director of the Information Technology and of the Certificates

After consultation of the Data Protection and of the Certificates

Being signed by the Director of the Information Technology and of the Certificates

Being signed by the Director of the Information Technology and of the Certificates

Being in conformity with the statutory provisions

Whereas

## GDPR



**THE PERSONAL DATA PROTECTION BILL, 2019**  
2019-2020

**AMENDMENTS**

**CHAPTER I**  
Preamble

1. Short title and commencement.

2. Application of Act to processing of personal data.

3. Definitions.

**CHAPTER II**  
Structure of Data Protection

4. Principles of processing of personal data.

5. Conditions or purposes of processing of personal data.

6. Conditions or collection of personal data.

7. Requirements of notice for collection or processing of personal data.

8. Quality of personal data processed.

9. Accountability or controller of personal data.

10. Accountability of data fiduciary.

11. Consent necessary for processing of personal data.

## PDP Bill



[http://www.mca.gov.in/section13/section13 amendment\\_act/20080205013.pdf](http://www.mca.gov.in/section13/section13 amendment_act/20080205013.pdf)

<https://pdr.info.in/>

<http://www.mca.gov.in/section13/section13 amendment/2019/201905013.pdf>



NPD  
Report



Report by the Committee of  
Experts on  
Non-Personal Data  
Governance Framework

<https://www.nrpa.gov.in/2020/11/04/committee-of-experts-on-non-personal-data-governance-framework/>



So, that is what we have, so we saw IT Act 2000, then we saw IT Act 2008 amendment, then we saw GDPR, PDP Bill and then the NPD report. Thanks again for listening to the class for week 11. Hopefully again this privacy laws gave you a different perspective of privacy as a topic and you are able to make some connections to other topics that you have already seen. Good luck, see you soon.