DPIIT IPR CHAIR
&
N.C.BANERJEE CENTRE FOR IPR STUDIES
NALSAR UNIVERSITY OF LAW, HYDERABAD

DEPARTMENT FOR PROMOTION OF INDUSTRY AND INTERNAL TRADE
MINISTRY OF COMMERCE & INDUSTRY,
GOVERNMENT OF INDIA

Data Protection & Privacy

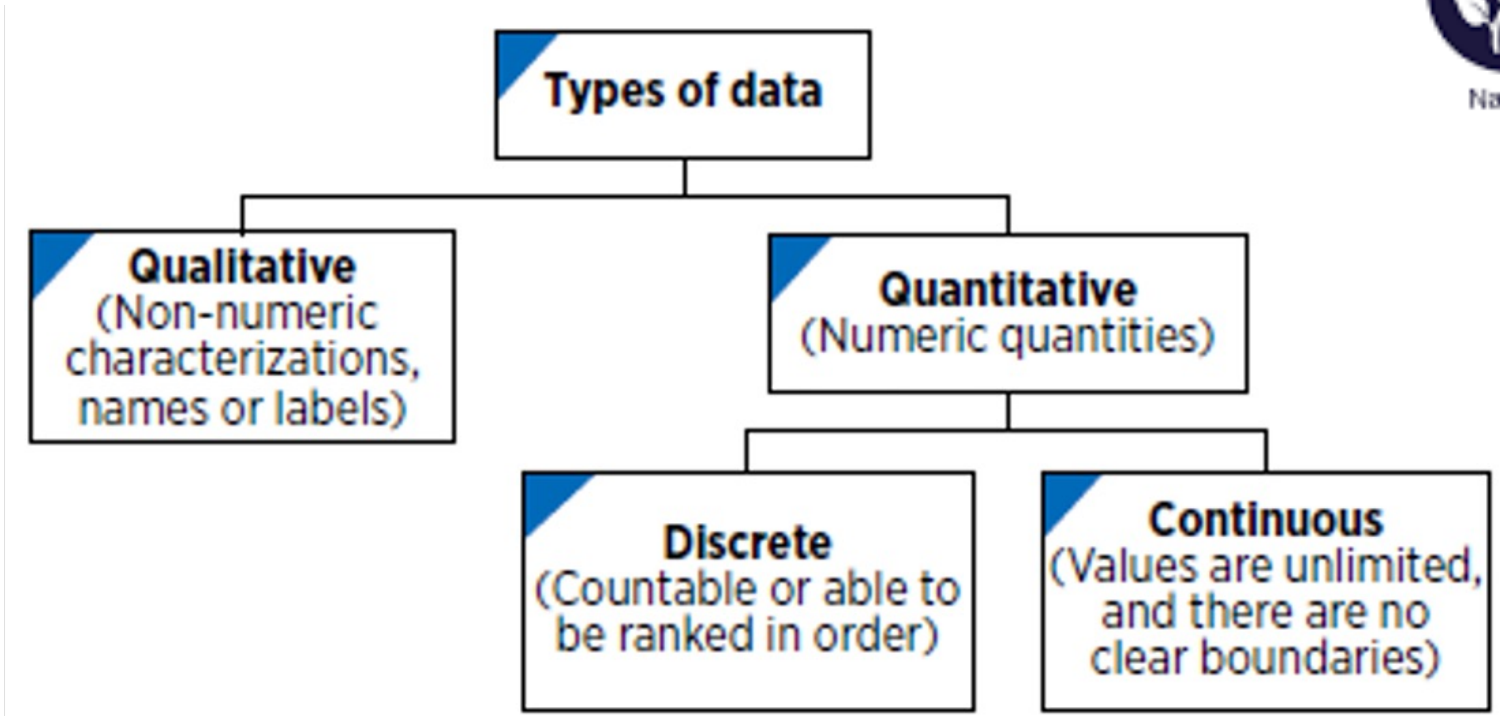
Techno Legal Issues

Advanced Diploma In Cyber Law
NALSAR University of Law, Hyderabad
Contact Class; April 2023.

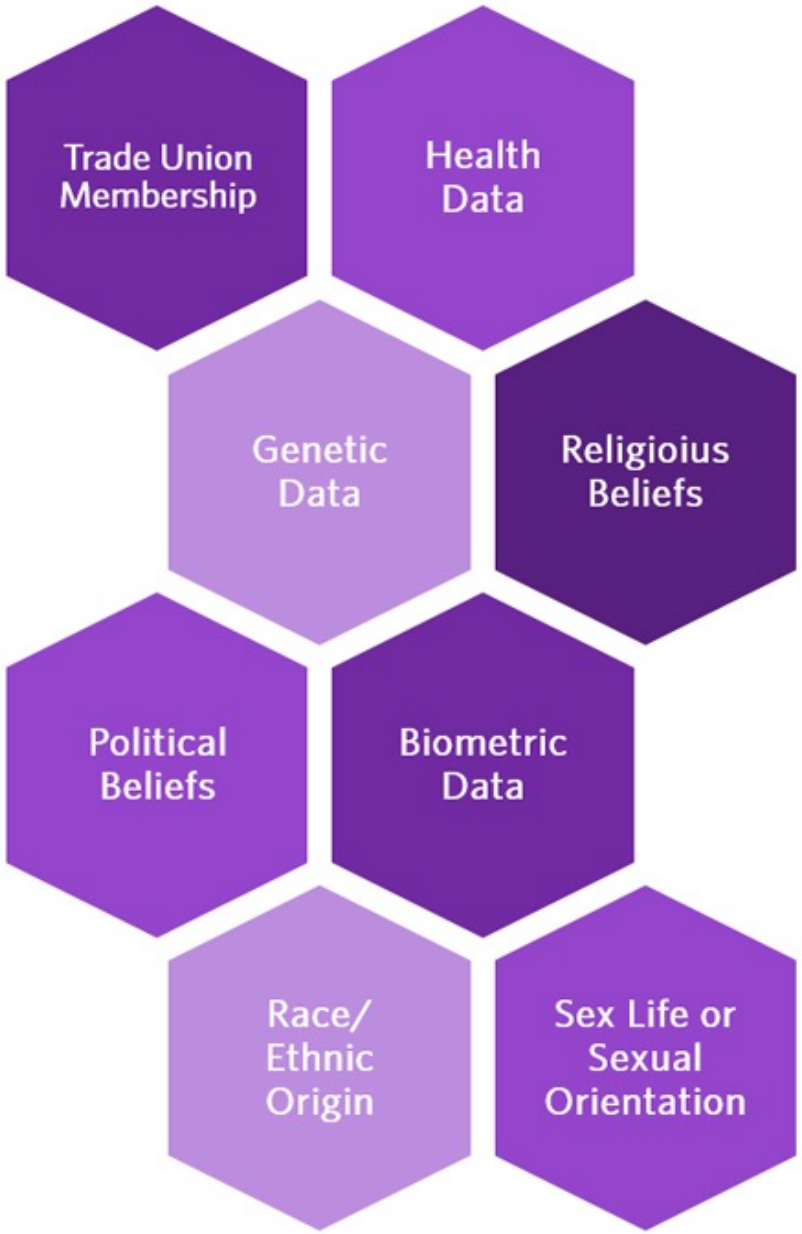
ANINDYA SIRCAR

Data

- Facts and statistics collected together for reference or analysis.
- A set of values of qualitative or quantitative variables about one or more persons or objects, while a datum is a single value of a single variable.



Personal Data



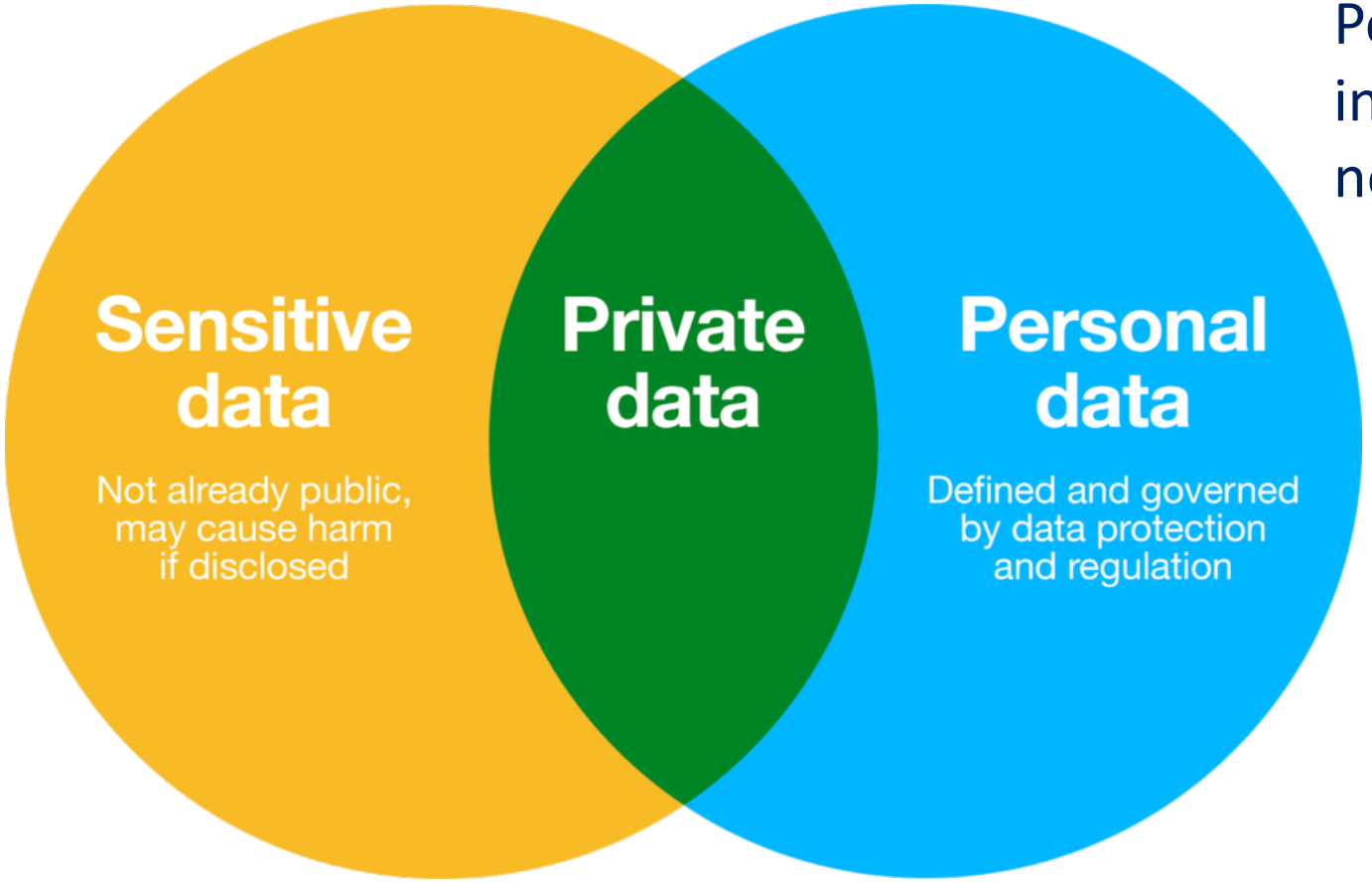
- Personal data is any information that relates to an identified or identifiable living individual.
- Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- Information about companies or public authorities is not personal data.
- *"Online identifiers"* includes IP addresses and *"cookie identifiers"* which may be personal data.

Personal Data - Private

The definition of personal information is very broad and it captures a large amount of information:

- a person's name, address, phone number or email address
- a photograph of a person
- a video recording of a person, whether CCTV or otherwise, for example, a recording of events in a classroom, at a train station, or at a family barbecue
- a person's salary, bank account or financial details
- allegations of wrongdoing against a person or details of wrongdoing or offences they may have committed
- details about a person's land ownership or disputes to do with their land
- details about a person's education or education activities, such as what degree they possess or their candidature for a PhD
- the fact that a person is a member, or leader, of an association and their attendance at meetings
- a person's medical details or health information
- a person's fingerprints or blood type
- details about a person's religious or sexual preferences
- details about a person's membership of a trade union or professional body.

Personal Data – Not Private



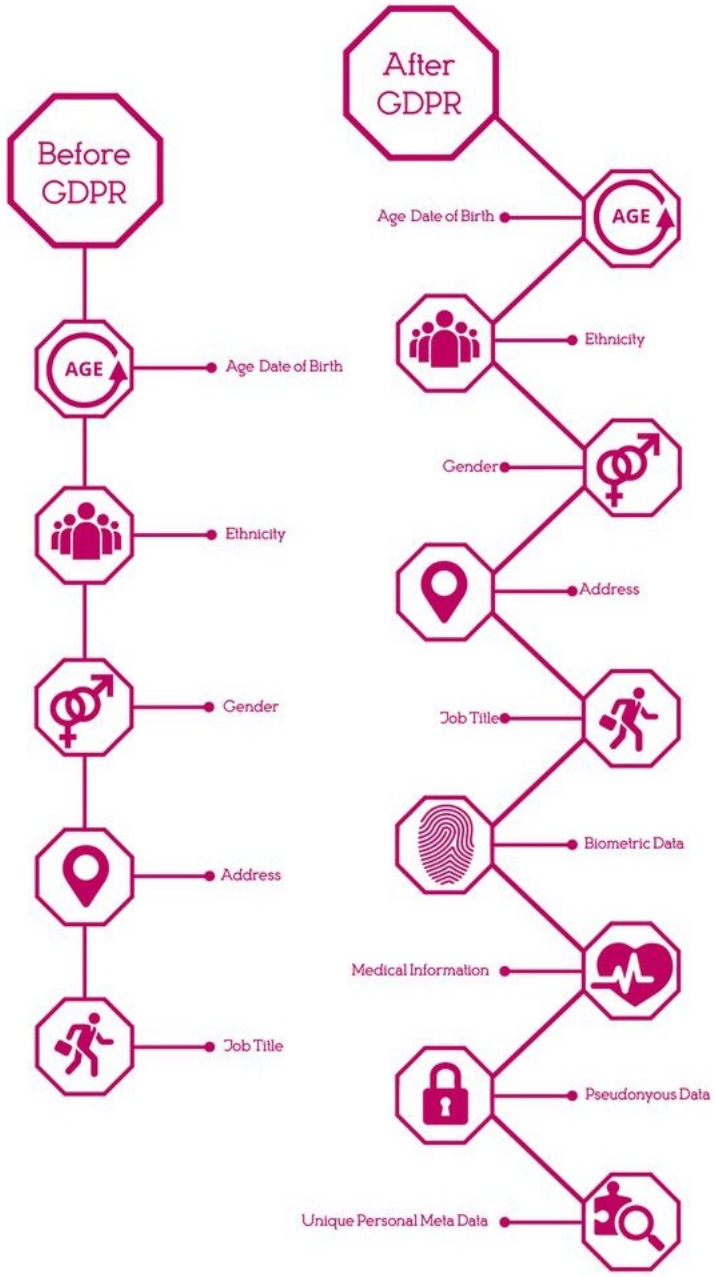
Personal information includes some information that people may not normally consider to be private:

- a work email address or phone number
- opinions given as part of a person's employment
- the fact that a person is the author of a report
- a person's name appearing in work documents
- a letter written in a person's official capacity, such as a letter from the president of a club.

GDPR

(General Data Protection Regulation)

- On May 25, 2018, the **European** General Data Protection Regulation (GDPR) came into effect.
- The political will behind and mandate of the GDPR were driven by the concern that individuals' personal information was being exploited in ways that undermined privacy and, by extension, democracy.
- It was intended to harmonize privacy and data protection laws across Europe while helping EU citizens to better understand how their personal information was being used, and encouraging them to file a complaint if their rights were violated.



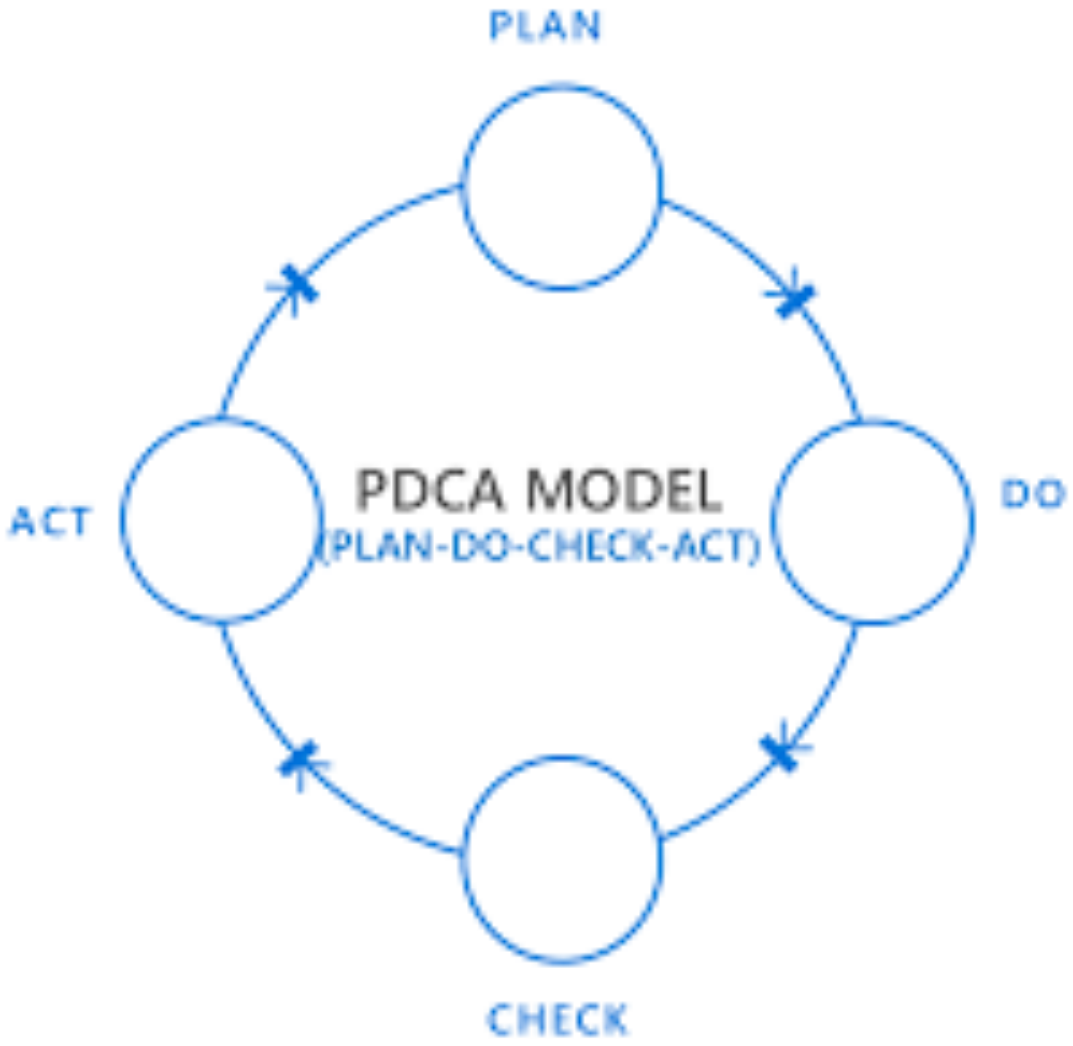
GDPR

(General Data Protection Regulation)

- Specific permission
  - Unless or until you give permission data can't be used for any other purpose or sell it to third parties.
- Privacy by design
  - Should not be asked for data that is not directly needed or relevant for the intended purposes.
- Data portability
  - Here right to ask for any data that a company has about you in a readable format.
- Right to be forgotten
  - Have a right to be forgotten and will be able to ask to delete your data.
  - Two exceptions are:
    - it will not apply to information that there is a legal requirement to keep; and
    - medical record where required.
- Definitive consent
  - There has to be a clear and affirmative consent before private data is processed.
- Information in clear readable language
  - The right of the individuals to get and read the information clearly.
- Limits on the use of profiling
  - Profiling will be allowed with the consent of the person concerned, where permitted by law or when needed to pursue a contract and requires human intervention.
- Everyone follows the same law
  - Everyone abides by the same rules to do business in the EU.
- One-stop solution
  - Only one regulatory body to do business in the EU.
- Adopting techniques
  - Promote techniques such as anonymization, pseudonymization and encryption.

GDPR

(General Data Protection Regulation)



Data Protection & Privacy - UK

Data Protection Act 2018

- The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.
- The Data Protection Act 2018 is the UK's implementation of the GDPR.
- Everyone responsible for using personal data has to follow strict rules called *'data protection principles'*
- They must make sure the information is:
  - used fairly, lawfully and transparently
  - used for specified, explicit purposes
  - used in a way that is adequate, relevant and limited to only what is necessary
  - accurate and, where necessary, kept up to date
  - kept for no longer than is necessary
  - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Data Protection & Privacy - UK

- There is stronger legal protection for more sensitive information, such as:
  - race
  - ethnic background
  - political opinions
  - religious beliefs
  - trade union membership
  - genetics
  - biometrics (where used for identification)
  - health
  - sex life or orientation
- There are separate safeguards for personal data relating to criminal convictions and offences.

- Under the Data Protection Act 2018, a UK citizen has the right to find out what information the government and other organisations store about one:
  - be informed about how your data is being used
  - access personal data
  - have incorrect data updated
  - have data erased
  - stop or restrict the processing of your data
  - data portability (allowing you to get and reuse your data for different services)
  - object to how your data is processed in certain circumstances
- One has rights when an organisation is using one's personal data for:
  - automated decision-making processes (without human involvement)
  - profiling, for example to predict your behaviour or interests

Data Protection & Privacy - US

- The US doesn't *(yet)* have a federal-level general consumer data privacy law, let alone a data security law - EU with its GDPR has both!
- However, the Californian Consumer Privacy Act (CCPA), does come close to addressing consumer data privacy at least for California residents.
- There is no single principal data protection legislation in the United States. Rather, a jumble of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of US residents.
- At the federal level, the Federal Trade Commission Act (15 USC § 41 *et. seq.*)
- The US has several sector-specific and medium-specific national privacy or data security laws, including laws and regulations that apply to financial institutions, telecommunications companies, personal health information, credit report information, children's information, telemarketing and direct marketing.
- The US also has hundreds of privacy and data security among its 50 states and territories, such as requirements for safeguarding data, disposal of data, privacy policies, appropriate use of Social Security numbers and data breach notification.

Data Protection & Privacy - US

- **US Privacy Act of 1974**
  - Right of US citizens to access any data held by government agencies. And a right to copy that data.
  - Right of citizens to correct any information errors
  - Agencies should follow data minimization principles when collecting data – least information *"relevant and necessary"* to accomplish its purposes.
  - Access to data is restricted on a need to know basis – for example, employees who need the records for their job role.
  - Sharing of information between other federal (and non-federal) agencies is restricted and only allowed under certain conditions
- **HIPAA** (Health Insurance Portability and Accountability Act, 1996)
  - To regulate health insurance.
- **GLBA** (Gramm-Leach-Bliley Act, 1999)
  - Protects non-public personal information, which is defined as any *"information collected about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available".*
- **COPPA** (Children's Online Privacy Protection Act, 2000)
  - Regulates personal information collected from minors.
  - Prohibits online companies from asking for personal information from children 12-and-under unless there's verifiable parental consent.

HIPAA

(Health Insurance Portability and Accountability Act)

- A US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.
- The main purposes of HIPAA
  - Privacy of health information,
  - Security of electronic records,
  - Administrative simplification,
  - Insurance portability.
- Provides detailed instructions for handling a protecting a patient's personal health information.

Data Protection & Privacy - US

State	*Right to Delete?*	*Right to Access?*	*Right to Correct?*	*Private Right of Private Action?*	*Broad Definition of PII?*	*Businesses covered*	*Status*
California	Yes	Yes	No	$750/consumer (breaches)	Yes (Probabilistic)	Revenues over $25 million	In effect : 01/01/2020
New York	Yes	Yes	Yes	$750/consumer	Yes	All	Pending
Maryland	Yes	Yes	No	No. (Only through AG.)	Yes (Probabilistic)	Over $25 million	Pending
Massachusetts	Yes	Yes	No	$750/consumer	Yes (Probabilistic)	Over $10 million	Pending
Hawaii	Yes	Yes	No	No	Yes	All	Pending
North Dakota	No	Yes	No	Limited	No	Over $25 million	Pending

INDIA: Existing Framework

- General Application
  - Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011
- Govt. Collection of Data
  - Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016
  - Aadhaar (Data Security) Regulations, 2016
- Banking Sector
  - Credit Information Companies (Regulation) Act, 2005
  - Credit Information Companies Regulations, 2006
  - Circulars of Reserve Bank of India including KYC circulars
  - Master Circulars on credit cards, etc.
  - Master Circulars on Customer Services
  - Code of Bank's commitment to Customers
- Telecom Sector
  - Unified License Agreement issued to telecom service providers by the Department of Telecommunications
  - Telecom Commercial Communication Preference Regulations, 2010
- Healthcare Sector
  - Clinical Establishments (Central Government) Rules, 2012
  - Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.

INDIA: Justice B N Srikrishna Bill

- The Government of India constituted a committee, chaired by Justice Srikrishna (retired), Supreme Court of India in August 2017 to design and draft data protection laws for India.
- The committee after a year of deliberations and public consultations has released a draft bill titled *'The Personal Data Protection Bill, 2018'* (Draft Bill).
- After further deliberations the Bill was approved by the cabinet ministry of India on December 04, 2019 as the **Personal Data Protection Bill 2019** and tabled in the Lok Sabha on December 11, 2019.

"Sensitive Personal Data" means personal data revealing, related to, or constituting, as may be applicable—

- passwords;
- financial data;
- health data;
- official identifier;
- sex life;
- sexual orientation;
- biometric data;
- genetic data;
- transgender status;
- intersex status;
- caste or tribe;
- Religious or political belief or affiliation; or
- any other category of data specified by the Authority under section 22.

INDIA: Personal Data Protection Bill, 2019

Decoding the data protection bill

WHAT IT MEANS FOR CONSUMERS

- **DATA** can be processed or shared by any entity only after consent.
- **SAFEGUARDS**, including penalties, introduced to prevent misuse of personal data.
- **ALL** data to be categorized under three heads—general, sensitive and critical.

THE GOVERNMENT & REGULATORY ROLE

- **GOVT** will have the power to obtain any user's non-personal data from companies.
- **THE** bill mandates that all financial and critical data has to be stored in India.
- **SENSITIVE** data has to be stored in India but can be processed outside with consent.

WHAT COMPANIES HAVE TO DO

- **SOCIAL** media firms to formulate a voluntary verification process for users.
- **SHARING** data without consent will entail a fine of ₹15 crore or 4% of global turnover.
- **DATA** breach or inaction will entail a fine of ₹5 crore or 2% of global turnover.

INDIA: Personal Data Protection Bill, 2019

DATA PRINCIPAL	• Only natural persons (not restricted to Indian citizens)
DATA FIDUCIARY	• Private entity or public entity or individual who determines the purpose and means of processing of personal data
DATA PROCESSOR	• Private entity or public entity or individual who processes personal data on behalf of data fiduciary (not an employee of data fiduciary)
TWO TYPES OF PERSONAL DATA	• 'Personal Data' and 'Sensitive Personal Data' • Personal Data has been defined to mean data relating to natural person, who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person • Sensitive Personal Data has been specifically defined to include, inter alia, passwords, financial data, health data, biometric data, genetic data, etc.
APPLICABILITY	• To data fiduciary or data processor in relation with personal data (not applicable on anonymised data or non-personal data)
TERRITORIALITY	• Extra-territorial in operation and is not restricted to Indian entities • Test is 'connection with any business carried on in India' or 'systematic activity of offering goods or services to data principals within India' or 'connection with activity which involves profiling of data principals within India'
EXEMPTIONS	• Security of the State; Prevention, detection, investigation and prosecution of contraventions of law; Processing for legal proceedings; Research, archiving or statistical purposes; Personal or domestic purposes; Journalistic purposes; Manual processing by small entities have been exempted from the application of the Draft Bill

INDIA: Personal Data Protection Bill, 2019

OBLIGATIONS OF DATA FIDUCIARY/ DATA PROCESSOR	• Fair and reasonable processing • Lawful processing • Purpose limitation • Collection limitation • Data quality • Data storage limitation • Accountability • Notice to data principal
GROUNDS FOR PROCESSING PERSONAL DATA	• Consent – free, informed, specific, clear and capable of being withdrawn • Functions of the State • Compliance with law or orders of court • For prompt action • For employment • For reasonable purposes
GROUNDS FOR PROCESSING SENSITIVE PERSONAL DATA	• Explicit consent • Similar to grounds for processing personal data
PERSONAL DATA OF CHILDREN	• Safeguards for processing personal data of children
RIGHTS OF DATA PRINCIPAL	• Right to confirmation and access • Right to correction • Right to data portability • Right to be forgotten

INDIA: Personal Data Protection Bill, 2019

TRANSPARENCY AND ACCOUNTABILITY MEASURES	• Privacy by Design • Personal Data Breach notification • Security Safeguards • Data Protection Impact Assessment • Record keeping and Data Audits • Data protection officer • Classification of data fiduciaries as significant data fiduciaries
TRANSFER OF PERSONAL DATA OUTSIDE INDIA	• Data localization by keeping one copy of personal data in India • Critical personal data (as notified) to be only processed in India • Personal data other than critical data may be transferred outside India on the basis of approved contractual clauses or to countries approved by the Indian regulator
DATA PROTECTION AUTHORITY	• Dedicated regulatory authority to be established to monitor implementation of the data protection obligations
REMEDIES	• Heavy penalties extending up to INR15 Crores (approximately USD 2,143,000) or 4% of total worldwide turnover of preceding FY
TRANSITIONAL PROVISIONS	• Notified data to be within 12 months from the date of enactment • Most provisions to be in force within 18 months from the notified date

Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors.

- A landmark judgment of the Supreme Court of India, which holds that the right to privacy is protected as a fundamental constitutional right under Articles 14, 19 and 21 of the Constitution of India.
- The constitutional foundations of the right to privacy were recognized in the judgement of a number of complaints against the UIDAI,
- The nine-judge bench unanimously held *that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".*
- It was held that the right to privacy is an intrinsic part of the fundamental right to life and personal liberty under Article 21 (in particular and in all fundamental rights in Part III which protect freedoms in general) of the Constitution of India.
- The Court recognised *'informational privacy'* as an important aspect of the right to privacy that can be claimed against state and non-state actors, but such a right is not an absolute right and may be subject to reasonable restrictions.
- The Court has laid down a test to limit the possibility of the State clamping down on the right, i.e., such an action must be sanctioned by law, it must be necessary to fulfil a legitimate aim of the State, the extent of the State interference must be *'proportionate to the need for such interference'* and there must be procedural safeguards to prevent the State from abusing its power.

WRIT PETITION (CIVIL) NO 494 OF 2012

Digital Personal Data Protection Bill, 2022

- MeitY had withdrawn Personal Data Protection Bill, 2019, owing to multiple recommendations received through public consultation. As revised version of its predecessor, the Government released Digital Personal Data Protection Bill on November 18, 2022.

- This bill is a part of a list of legislations that includes:
  - IT rules,
  - National Data Governance Framework Policy and
  - Digital India Act.

- Key highlights of this bill include:
  - Applicable to digitized data
  - Providing itemized notice and to be accessible in English or any other languages mentioned in the constitution of India
  - Penalty for non-compliance up to INR 500 crores
  - Deemed consent
  - Right to nominate as a data subject right and many more.

- Obligations such as data localization and privacy by design are omitted

- There are certain open-ended requirements in the bill which could play an important role in determining the future of data protection.

- Provides greater emphasis and encourages organisations to digitize personal data.

National Data Governance Framework Policy, 2022

- MeitY released the draft National Data Governance Framework Policy on May 26, 2022, inviting the public to provide feedback and comments on the same.

- The key objectives of the Policy are as follows:
  - To accelerate Digital Governance with standardized data management and security standards across the government;
  - To set quality standards, have standard API's and tech standards for management and access of government data and promote expansion of the Indian Datasets Program and non-personal datasets ecosystem;
  - To promote ownership, accountability and transparency in non-personal data and datasets access, providing for sharing of non-personal data only via platforms designated and authorized by IDMO (*defined below*);
  - To build a platform which would allow the receipt and processing of dataset requests;
  - To construct digital government goals and capacity, competency and knowledge in government departments and entities;
  - To create uniform standard based public digital platforms while ensuring privacy, safety and trust of citizens regarding their data;
  - To ensure that citizens are more aware and accordingly have increased participation and engagement with the government.

National Data Governance Framework Policy, 2022

- The Policy is applicable to all such data which is collected and managed by government departments and entities; thus bringing all government departments under its ambit.

- Even state governments are encouraged to adopt the provisions of this Policy, as may be applicable.

- The Policy is also applicable to non-personal datasets as it proposes to launch an **'India Datasets Program'** which is based on non-personal data.

- The Policy provides certain rules and methods which would ensure that any anonymized data and non-personal data from both the private or government entities can be accessed by the 'research and innovation eco-system', in a safe and accessible manner.

- The Policy provides for setting up of an India Data Management Office **(*IDMO*),** within the Digital India Corporation (**"*DIC*"**) under MEITY, which would primarily be responsible for framing, managing, reviewing and revising the Policy; as well as for developing guidelines, standards and rules under the Policy.

- For effective implementation of the Policy, the IDMO will closely coordinate with the **'Chief Data Officers'** of the Data Management Units (**DMU)** which is set up under every department and ministry of the government and will also provide assistance to all the State-level Data Officers appointed by the State governments.

Digital India Act, 2023

- DIA is aimed at completely overhauling the country's existing Information Technology Act 2000 (IT Act), and make way for a comprehensive and dynamic legislation to regulate digital technologies.

- MeitY, on March 09, 2023, organised a consultation to apprise representatives of the legal and technology industry amongst others, about the broad framework and core tenets of the DIA.

- Key components:
  - Enabling an open internet.
  - Enhanced obligations for intermediaries and other entities on the internet
  - Safe harbour principle under the DIA
  - Ensuring online safety and trust
  - False information
  - Regulating artificial intelligence
  - Regulation for privacy invasive devices
  - Enhanced penalties for cyber-crimes
  - Adjudicatory mechanism

- DIA holds great potential to accelerate India's growth and development in the digital age.

thank you

NALSAR University of Law
Justice City, Shameerpet, Medchal District, Hyderabad - 500101