Corporate Professionals

The Digital Personal Data Protection Act, 2023

Corporate Professionals

History

History of Privacy: *"As old as humankind itself"*

Privacy: "A Historical Perspective"

- Privacy as a recognized right emerged in the 19th and 20th century.
- However, the concept of privacy dates back to ancient societies.
- Even ancient texts like the Bible contain early examples of privacy violations and their consequences.
- The concept of privacy originates from the distinction between "private" and "public" spheres.
- Privacy is intricately linked to technological advancements.
- Today, rapid developments in science and technology have heightened privacy concerns.
- Laws need to evolve to address these modern challenges.

Historical Influences on the Right to Privacy

- Modern privacy as we know it today, originated from the 1890 study titled "The Right to Privacy" by Louis Brandeis and Samuel Warren.
- The study argued that individuals have the right to be left alone and protected from unwanted intrusion into their personal lives.
- The study created a foundation for privacy law and has had a significant impact on the development of privacy rights in the United States and around the world.
- They identified two phenomena as threats to privacy: technological advances, and the growing sensationalism of gossip in newspapers.

International Footing

- International human rights conventions recognize the right to privacy at both universal and regional levels.
- Key provisions include Article 12 (Universal Declaration of Human Rights), Article 17 (International Covenant on Civil and Political Rights), Article 8 (European Convention on Human Rights), and Article 7 (Charter of Fundamental Rights of the European Union).
- These provisions establish privacy as a fundamental human right, protecting private and family life, home, and correspondence.
- However, they lack detailed guidance on the scope of privacy and what aspects should be legally protected.
- Court decisions and case law play a crucial role in defining and applying privacy rights within these conventions

Corporate Professionals

Understanding Privacy in the Indian Context

Privacy in the Indian context

- The significance of safeguarding personal data can be traced to the landmark Supreme Court case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, 2017 SCC Online SC 996, decided on 24 August 2017.

- In this Landmark case, a nine-judge bench of the Supreme Court of India upheld the "Right to Privacy" as a fundamental right enriched under Article 21 of the Indian Constitution.

- The decision in question has played an influential role in laying the groundwork for the development of comprehensive laws concerning the importance of protecting personal data in India in accordance with privacy rights.

Exceptions

- However, the Hon'ble Supreme Court also observed that the right to privacy is not an absolute right. The Right to privacy falls in Part III of the Constitution and can be restricted in certain circumstances, such as national security or public interest.

- Privacy has both negative and positive aspects; it restricts the state from intrusion and obligates the state to protect and safeguard individual privacy rights.

- The Court has established a three-fold requirements that must be met before invading an individual's personal liberty;

i. Legality, which necessitates the presence of a law
ii. Need, defined by the legitimate state objective
iii. Proportionality, ensuring a logical reasoning between an action and effect

Journey of Data Protection Bill 2018 to Data Protection Act, 2023

- The committee, led by Justice B. N. Srikrishna, was constituted by the Central Government (Ministry of Electronics & Information Technology) on July 31, 2017.
- In the meanwhile, on 24 August 2017, Supreme Court acknowledged "privacy" as a fundamental right in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, 2017 SCC Online SC 996.
- The process began with the release of a white paper on the Data Protection framework for India by the Justice B. N. Srikrishna Committee on November 27, 2017.
- The Srikrishna Committee submitted their Draft Personal Data Protection Bill 2018 to the Ministry of Electronics and Information Technology (Meity) (Bill of 2018) on July 27, 2018.

Journey of Data Protection Bill 2018 to Data Protection Act, 2023

- Subsequently, the Personal Data Protection Bill 2019 (Bill of 2019) was introduced in the Lok Sabha on December 11, 2019.
- The same Bill was referred to the Joint Parliamentary Committee (JPC) on December 17, 2019, for further review.
- Following the outbreak of COVID-19, the JPC presented its report, along with suggested revisions to the 2019 Bill, in Parliament on December 16, 2021.
- However, on August 3, 2022, the Data Protection Bill of 2019 was withdrawn from Parliament, marking a significant development in the legislative process.
- Subsequently, the Draft of the Digital Personal Data Protection Bill 2022 was released on November 18, 2022, and was open for public consultation until December 17, 2022.

Enactment of the Digital Personal Data Protection Act, 2023

- On July 5, 2023, the Cabinet approved the Digital Personal Data Protection Bill 2023.
- The Digital Personal Data Protection Bill, 2023 was presented in Lok Sabha on August 3, 2023, by the Minister of Electronics & Information Technology and has been approved by the Parliament.
- The Lok Sabha approved the bill on August 7, 2023, followed by unanimous approval by the Rajya Sabha on August 9, 2023.
- The bill received Presidential assent on August 11, 2023, and was published in the official gazette
- The bill was subsequently published in the official gazette, officially becoming the Digital Personal Data Protection Act of 2023, and establishing a comprehensive framework for data protection in India

Corporate Professionals

Objective

Objective of the DPDP Act, 2023

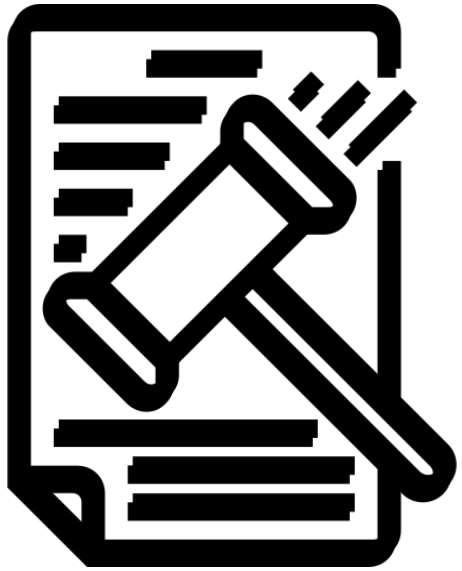
"The Act provides for the processing of digital Personal Data in a manner that recognizes both the rights of the individuals to protect their Personal Data and the need to process such Personal Data for lawful purposes and matters connected therewith or incidental thereto."

- The statement outlines the dual objectives:
  - to protect individuals' rights regarding their personal data
  - also recognizing the legitimate need to process that data for lawful purposes.
- The core objective of the Act is to create a thorough framework and put it in place for the protection and processing of personal data.

Corporate Professionals

Key Terminologies

Key Terms and Their Definitions



- **"Board"** means the Data Protection Board of India established by the Central Government under section 18 of this Act
- **"Consent Manager"** means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform
- **"Data"** means a representation of information, facts, concepts, opinions or instruction in a manner suitable for communication, interpretation or processing by human beings or by automated means
- **"Data Fiduciary"** means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data

Key Terms and Their Definitions

- **"Data Principal"** means the individual to whom the personal data relates and where such individual is—
  - a child, includes the parents or lawful guardian of such a child
  - a person with disability, includes her lawful guardian, acting on her behalf
- **"Data Processor"** means any person who processes personal data on behalf of a Data Fiduciary
- **"Digital Personal data"** means personal data in digital form
- **"Personal data"** means any data about an individual who is identifiable by or in relation to such data
- **"Significant Data Fiduciary"** means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10 of this Act

Key Terms and Their Definitions

- **“Personal Data Breach”** means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data
- **“Processing”** in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, storage, recording, organizing, sharing, alignment or combination…
- **“She”** refers to an individual, irrespective of gender

(Using "she" instead of "he" in parliamentary language marks a recognition of women's involvement and representation in law-making)

Corporate Professionals

Applicability

Applicability of the Act

As per Section 3 of the DPDP Act, 2023, this act applies to

- ***Digital Personal Data-***

The DPDP Act exclusively covers digital personal data, including data collected in digital form or non-digital data that has been digitized afterwards within the territory of India.

- ***Overseas applicability-***

The DPDP Act applies to digital personal data processed outside India only when such processing is associated with any activity linked to the provision of goods or services offered to Data Principals within India.

Non-Applicability

The Data Protection Act of 2023 specifies certain situations to which this act does not apply:

(i) When personal data is processed by an individual for any personal or domestic purpose

(ii) When personal data is made publicly available by the data principal herself or any other person under a legal obligation.

Corporate Professionals

Legal Grounds for Processing Personal Data

Grounds For Processing Personal Data

- ***As Per Section 4 of the Data Protection Act, 2023 –***

A person can process the personal data of a Data Principal, in accordance with this act, for a lawful purpose only after obtaining "**Free consent**" from the Data Principal or processing for **"certain legitimate use"**.

Here, 'lawful purpose' refers to any purpose not expressly prohibited by law.

Corporate Professionals

Notice

Role of Notice

As Per Section 5 of the Data Protection Act, 2023

- Data fiduciaries are required to make a request to the Data Principal for consent along with a clear and detailed notice, in a manner prescribed by the government by way of rules, regarding the personal data to be processed and the purpose(s) of processing.
- Data principals also must be informed of their right to withdraw consent and the grievance redressal procedure made available by the data fiduciary and a right to make a complaint to the Board.
- Such notice must be made accessible in English and in all 22 languages specified in the Eighth Schedule of the Constitution.

Corporate Professionals

Consent

Free Consent

As per Section 6 of the Data Protection Act, 2023

- Such consent has to be freely given, specific, informed, unconditional, and unambiguous, with a clear and affirmative action.
- In accordance with Section 5, a notice is required from the data fiduciary to the data principal prior to seeking consent.
- The notice should contain details about the personal data to be collected and the purpose of processing.
- Consent may be withdrawn, reviewed and managed at any point in time through a Consent Manager and cease of data by a Data Fiduciary within a reasonable time.

Corporate Professionals

Exemptions from Data Principal Consent

Certain Legitimate Use

As per section 7 of the Data Protection Act, 2023

- Consent of the Data Principal will not be required for 'legitimate uses' including:

(i) specified purpose for which data has been provided by an individual voluntarily

(ii) provision of benefit or service by the government

(iii) medical emergency

(iv) employment.

(v) to comply with any judgment, decree and order issued under any law

(vi) to safeguard and assist individuals during disasters or public order breakdowns

Corporate Professionals

Parental Consent

Parental Consent for Processing of children's personal data

- The Act defines a child as an individual under the age of 18.
- As per section 9 of this act, Processing of children's data (below 18 years) or data of a person with a disability unable to give consent, under the DPDP Act, requires verifiable consent from parents or lawful guardians.
- The DPDP Act also restricts data fiduciaries from engaging in tracking, behavioural monitoring, and direct targeted advertising at them or causing a detrimental effect on their well-being.

Corporate Professionals

Obligations of Data Fiduciary and Significant Data Fiduciary

Obligation of Data Fiduciary

As per Section 8 of the Data Protection Act, 2023, data fiduciaries have certain responsibilities and obligations to comply with the provisions of the Act. Some general obligations of data fiduciaries are:-

- To engage, appoint or involve a Data Processor to process personal data under a valid contract only.
- To comply with all the provisions of the Act and ensure the accuracy, consistency and completion of data.
- Build reasonable security safeguards and organizational measures to prevent a data breach.
- Intimation to the Board and affected data principals in the event of a data breach.

Obligation of Data Fiduciary

- Obligation to erase personal upon the intended purpose being served or completed.
- Data fiduciaries are required to delete personal data if the data principal withdraws their consent
- Establishment of a grievance redressal mechanism to redress the Data Principal's grievances.
- In case the Data fiduciaries processing personal data of children or disabled individuals must ensure that the data processing does not adversely affect the well-being of the child and must abstain from conducting behavioural monitoring or tracking of children after obtaining the verifiable parent consent.

Significant data fiduciary

- The Data Protection Act of 2023, as per section 10, empowers the Government to designate or classify any data fiduciary (or a class of data fiduciaries) as a 'Significant Data Fiduciary' ("SDF") in consonance with an assessment of such relevant factors prescribed under the Data Protection Act.

- Organizations which deal with large volumes of individual personal data (banks, telecom companies, insurance companies, OTT streaming companies)

Additional obligations of significant data fiduciaries

- Appoint a data protection officer based in India
- Appoint an independent data auditor
- To conduct periodical audit
- Conduct data protection impact assessments (a process to assess the risk to the rights of data principals).

Corporate Professionals

Rights and Duties of Data Principal

Rights of Data Principal

The Data Protection Act of 2023 grants specific rights to Data Principals under Chapter III

- An individual whose data is being processed (data principal) will have certain rights

(i) Right to Obtain information about personal data under section 11 of the Act

(ii) Right to Seek correction and erasure of personal data under section 12 of the Act

(iii) Right to Nominate another person to exercise rights in the event of death or incapacity under section 13 of the Act

(iv) Right to Raise a Grievance and redressal under section 14 of the Act

Duties of Data Principal

- **Additionally, the Act imposes specific responsibilities/duties on data principals under section 15 of the Act.**

(i) To comply with all the provisions of the act and all applicable laws while exercising rights

(ii) Not to register a false or frivolous complaint and grievances with the Board

(iii) Not to furnish any false particulars or impersonate another person in specified cases.

(iv) Not to suppress any material information while furnishing personal data

(v) Violation of duties by the data principal will be punishable with a penalty of up to Rs 10,000.

Corporate Professionals

Cross-border Transfer of Data

Processing of Personal Data outside India

- The Cross-border transfer of personal data outside India is allowed to countries/territories unless the Government restricts such transfer through notification.
- Nevertheless, it's important to note that the DPDP Act specifies that its provisions complement and do not override any existing laws. This means that other regulations related to the cross-border transfer of data may also apply.

- ***The Securities and Exchange Board of India*** issued a circular in March 2023 with respect to adopting cloud services. Regulated entities must ensure that data is processed within India's legal jurisdiction, subject to certain conditions.
- ***The Reserve Bank of India*** issued a directive in April 2018 with respect to data localization regulations and payment system data must be stored only in India.

Corporate Professionals

Exemptions

Exemptions

The Act includes specific exemptions outlined in Section 17 under which certain provisions of the act may not apply.

- To enforce any legal right or claim.
- Necessary to process such data for carrying out functions of any courts, judicial and quasi-judicial bodies.
- Where it is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law. Processing of personal data of an Indian-based individual outside the territory of India in furtherance of any contract with a Foreign Individual.
- Processing of such data is necessary for a scheme of mergers and amalgamation, corporate restructuring, etc., approved by a court.
- To know the whereabouts and financial information of any person who has defaulted in payments due to Financial Institutions.

Corporate Professionals

Establishment of the Data Protection Board & Key Functions

Data Protection Board of India

- The central government in accordance with Chapter V, section 18 of the Act, will establish the Data Protection Board of India, consisting of a chairperson and other members.
- Board members will be appointed for two years and will be eligible for re-appointment.
- The central government will prescribe details such as the number of members of the Board and the selection process.
- Appeals against the decisions of the Board will lie with TDSAT

Key functions of the Board, as outlined in section 27 of the Act

- **Managing Data Breaches:** The Board is responsible for taking immediate actions in response to personal data breaches, conducting investigations, and imposing penalties as per the Act.
- **Investigating Complaints:** The Board investigates complaints from Data Principals about data breaches, violations of Data Fiduciary obligations, or infringements of Data Principals' rights. It can also act on referrals from government authorities or court orders.
- **Supervising Consent Managers:** The Board can inquire into breaches of personal data obligations by Consent Managers based on Data Principals' complaints and impose penalties.

Key functions of the Board, as outlined in section 27 of the Act

- **Regulating Consent Managers:** The Board can investigate breaches of Consent Managers' registration conditions and impose penalties when violations occur.
- **Enforcing Intermediary Obligations:** The Board can investigate breaches of section 37(2) by intermediaries when referred by the Central Government and impose penalties.
- **Issuing Directives:** The Board can issue directives to ensure effective implementation of the Act. Failure to comply with these directives may result in penalties.
- **Modifying or Canceling Directives:** The Board can modify, suspend, withdraw, or cancel directives issued to individuals or entities. It may also impose conditions when making such changes based on representations or referrals

Corporate Professionals

Appeals, ADR and Jurisdiction

Appeals

- The Appeals against the decisions of the Data Protection Board shall, as per Section 29 of the Digital Data Protection Act, 2023, lie with the Telecommunications Dispute Settlement and Appellate Tribunal (TDSAT) established under the Telecom Regulatory Authority of India Act, 1997 (TRAI Act).

- The prescribed time limit for preferring an appeal is strictly sixty (60) days from the date of receipt of the Board's decision.

- Further, the Orders passed by TDSAT are appealable before the Hon'ble Supreme Court as per Section 18 of the TRAI Act

Section 31: Empowering the Board to Mandate "Alternative Dispute Resolution"

- In the event that the Board believes that a complaint can be resolved through mediation.
- The Board has the authority to instruct the involved parties to seek a resolution through mediation.
- The parties involved have the option to choose a mediator they both agree on.
- Otherwise, they can follow the mediation process prescribed by existing Indian laws.

Jurisdiction

- Civil courts are prohibited from entertaining any lawsuits or legal proceedings related to any matters within the authority of the Board as granted under section 39 of the Data Protection Act, 2023.

- Moreover, no court or authority is permitted to issue injunctions to halt actions taken or planned in accordance with the powers vested in the provisions of this Act.

Corporate Professionals

Power to make rules

The Central Government is empowered to make rules

In accordance with section 40 of this Act, for the purpose of implementing the Act. Power to make rule on

- Informing Data Principals by Data Fiduciary
- Obligation and Accountability of Consent Manager
- Reporting of Personal Data Breach to the Board
- Furnishing details of Data Protection Officers
- Reporting Personal Data Breaches to the Board
- Verifiable consent and processing of Children's Personal Data
- Timeframe for Data Fiduciary to respond to grievances
- Appointment and service term of the chairperson and other member of the Board
- Salary, Allowances and terms of service
- Procedure for dealing with appeals

Corporate Professionals

Penalties

Penalties

Non-compliance with the DPDP Act can result in monetary penalties ranging from INR 10,000 to INR 250 crores, depending on the violation.

Penalties for non-compliance under The Schedule of Data Protection Act, 2023

S. No.	Non-compliance	Maximum penalty in INR
1.	Failure to take security measures to prevent data breaches under section 8 sub-section 5	250 crores
2.	Failure of data fiduciaries to notify data breaches under section 8 sub-section 6	200 crores
3.	Non-fulfilment of obligations to processing of children's data under section 9	200 crores
4.	Breach in observance of a significant data fiduciary's obligations under section 10	150 crores
5.	Breach in observance of a data principal's obligations under section 15	10,000
6.	Breach of the terms of a voluntary undertaking accepted by the Board under section 32	Up to the penalty which may be applicable for the breach for which the voluntary undertaking was submitted
7.	General non-compliance of the DPDP Act	50 crores

Corporate Professionals

Impact of the Act

Impact on the Education Institutes

- –The New DPDP Act, 2023, will apply to an institute that collects personal data during enrollment, identification, recordkeeping, and payment processing.

- **Obligations** – The obligation of an institution will be:
  - to provide notice to the data principal,
  - secure consent (verifiable parental consent in case the data principal is a child or disability to provide consent),
  - and uphold accuracy and consistency.

Impact on Social Media

- This Act will apply when personal data is processed for purposes including but not limited to user registration, personalization, personalized and targeted advertising, content preferences, and third-party service provision. However, this act will not apply when personal data is intentionally made public by a Data Principal.

- **Obligations** –
  - To provide notice to the data principal, obtain consent (verifiable parental consent in case the data principal is a child or disability to provide consent)
  - Maintain accuracy and consistency.
  - Erasure of personal data upon withdrawal of consent or purpose is met, and not to track behavioural monitoring and target advertisement at children, the appointment of Data Protection Officer and independent auditor, and Periodical compliance checks.

Impact on Banking, Financial Services and Insurance

- This Act will apply when these companies collect or store data during user registration, payment details, transactions, Know Your Customer (KYC) details, and Insurance claims process.

- **Obligations** –
  - Provide data principals with an easy way to communicate and make requests.
  - Erasure of data upon the withdrawal of the consent or purpose is met.
  - Enforcing a data processor contract in case of engaging a third party to maintain data and to comply with the existing law in force concerning data localization.

Impact on OTT Streaming Services

- This Act will apply when these OTT streaming companies collect or store data during user registration, payment details, transactions, content preferences and communications.

- **Obligations** –
  - Provide notice, obtain consent or verifiable consent
  - Erasure of data upon the withdrawal of the consent or purpose is met
  - Not to track behavioural monitoring and target advertisement at children
  - As a Significant Data Fiduciary, the appointment of a Data Protection Officer and independent auditor and periodical compliance checks
  - And adherence to the government's direction concerning public information

Impact on E-Commerce

- This Act applies when an e-commerce website processes personal during when services are rendered to the Data Principal. Data may be collected while signing up, making purchases, redirecting services, processing payments, and engaging with customer support.

- **Obligations** –
  - Provide notice, obtain consent or verifiable consent
  - Erasure of data upon the withdrawal of the consent or purpose is met
  - Provide data principals with an easy way to communicate and make requests.
  - Not to track behavioural monitoring and target advertisement at children
  - And adherence to the government's direction concerning public information

Corporate Professionals

GDPR v/s DPDP

GDPR versus India’s Data Protection Act, 2023

- The General Data Protection Regulation (GDPR) is a set of rules and regulations enacted by the European Union (EU) and applied in the European Economic Area (EEA) to protect information privacy. It imposes significant fines for non-compliance, with penalties that can reach up to EUR 20 million or 4% of a company's global annual turnover, whichever is higher.

- The GDPR grants various rights to individuals, including the right to access, correct, delete, limit processing, transfer data, and object to data processing.

- Additionally, it establishes fundamental principles for handling personal data, including fairness, transparency, purpose limitation, minimal data collection, accuracy, data storage limits, data security, and accountability. These principles ensure responsible and ethical treatment of personal data while upholding individuals' privacy rights.

Countries

- **The GDPR has been implemented in the following 27 countries:**

• Austria • Belgium • Bulgaria • Croatia • Cyprus • Czech Republic • Denmark • Estonia • Finland • France • Germany • Greece • Hungary • Ireland • Italy • Latvia • Lithuania • Luxembourg • Malta • The Netherlands • Poland • Portugal • Romania • Slovakia • Slovenia • Spain • Sweden • United Kingdom

- **Although the following countries are in Europe, they have not adopted the GDPR regulation:**

• Albania • Belarus • Bosnia and Herzegovina • Kosovo • Moldovia • Montenegro • North Macedonia • Russia • Serbia • Turkey • Ukraine

Countries with their respective laws

Here is a list of countries and regions along with their respective data protection laws similar to GDPR:

- Switzerland (Personal Data Protection Law)
- Bahrain (Personal Data Protection Law)
- Israel (Data Security Regulations)
- Qatar (Law No. 13)
- Turkey (Law on Protection of Personal Data No. 6698)
- Kenya (Data Protection Act)
- Mauritius (Data Protection Act)
- Nigeria (Data Protection Regulation)

Countries with their respective laws

- South Africa (Protection of Personal Information (POPI) Act)
- Uganda (Data Protection and Privacy Act, 2019)
- Japan (Act on the Protection of Personal Information)
- South Korea (Personal Information Protection Act)
- New Zealand (Privacy Act)
- Argentina (Personal Data Protection Act No 25,326)
- Brazil (General Data Protection Law LGPD)
- Uruguay (Act on the Protection of Personal Data and Habeas Data Action)
- Canada (Personal Information Protection and Electronic Documents Act (PIPEDA)

Difference

Tabular Difference of Data Principal Rights Between GDPR and the Data Protection Act

S. No.	Data Principal Rights	GDPR	Data Protection Act, 2023
1.	Right To Access	Yes	Yes
2.	Right to Rectification	Yes	Yes
3.	Right to Erasure	Yes	Yes
4.	Right to Data Portability	Yes	NO
5.	Right to Nominate	No	Yes
6.	Right to Grievance Redressal	No	Yes

Material Differences

- **Classification of Data:**
  1. GDPR classifies personal data into specific subsets with separate compliance requirements.
  2. DPDP does not classify personal data into separate categories, it applies equally to all digital personal data.
- **Applicability to Offline Data:**
  1. GDPR applies to both digital and offline data that is part of a filing system.
  2. DPDP Act restricts its applicability to digital or digitized data, excluding offline data.

Material Differences

- **Children's Data:**
  1. DPDP prohibits behavioral monitoring or targeted advertising aimed at children and requires verifiable parental consent.
  2. GDPR does not expressly prohibit such practices and lacks an explicit broad prohibition on data processing that may harm a child's well-being.
- **Grievance Redressal:**
  1. DPDP requires data subjects to seek redress from the data controller before complaining to the authority or courts.
  2. GDPR does not have this specific requirement, allowing data subjects to complain directly to the Supervisory Authority or courts.

Material Differences

- **Notice Requirements:**
  1. DPDP requires notice only when consent is the basis for data processing and not for legitimate uses.
  2. GDPR requires notice whenever data is collected from the data subject, not limited to consent scenarios.
- **Transfer of Data to Other Jurisdictions:**
  1. DPDP allows the Central Government to restrict the transfer of personal data to notified countries or territories outside India.
  2. GDPR regulates international data transfers with mechanisms like Standard Contractual Clauses and Binding Corporate Rules but does not provide for government restrictions on transfers

Corporate Professionals

Key Takeaways

Corporate Professionals

THANK YOU