1 1 MAY 2025

# NATIONAL LAW UNIVERSITY, JODHPUR

**End Term Examination – April – May, 2025**

**Semester: U.G. VIII Semester**

**Subject: Comparative Privacy & Data Protection Law (Optional)**

**Time: Three Hours** **Marks: 100**

***Instructions:***
1. ***All questions carry equal marks.***
2. ***Kindly answer any five out of six questions.***

Q 1) FunRealm Studios GmbH, a gaming company headquartered in Berlin, Germany, has developed a popular online multiplayer game called "MythQuest Arena." The game is widely played by children aged 10–17 across Europe and India. While the company claims to comply with applicable data protection regulations, recent investigations have raised concerns about its data processing practices involving minors.

It has come to light that:

- MythQuest Arena collects a wide range of personal data from users, including location data, browsing behaviour within the game, in-game choices, and time spent online.
- The game uses third-party trackers and in-house profiling tools to monitor children's preferences and behavioural patterns.
- Based on these insights, the company displays highly personalized advertisements, some of which promote in-game purchases and premium upgrades.
- Although the company offers a generic privacy policy, it does not clearly distinguish its practices for underage users.

Several digital rights organizations and child welfare groups in both Europe and India have raised objections to the company's practices, alleging violation of children's informational autonomy and best interests. You are an expert in data protection law. The company has approached you for legal advice in respect to these issues pertaining to the processing of personal data in India and the European Union. Support your analysis with reference to relevant provisions of the GDPR and DPDPA, as well as applicable case law or regulatory guidance where relevant

(Marks 20)

Q 2) Riva Sen, a university student in the State of Nyaya Pradesh, had been enrolled in a reputed institution when she entered into a consensual relationship with a fellow student, Anay Mathur. During their relationship, Riva had shared several intimate images and videos with Anay, on the understanding that these would remain private. Following a bitter breakup, Anay uploaded these materials onto several social media platforms and adult content websites without Riva's consent, tagging her full name and university affiliation.

Despite repeated complaints to the platforms, the content remained accessible for several weeks and was widely circulated. Riva faced immense mental distress, harassment from peers, and was forced to withdraw from the university. She later filed a complaint under the provisions of the Information Technology Act and the Penal Code of the country relating to cyberstalking, voyeurism, and transmission of obscene content.

During the proceedings, Riva also moved the High Court of Nyaya Pradesh, seeking an order to direct all websites and intermediaries to permanently delete the content, de-index any search results containing her name linked to such material. The websites opposed this plea on the grounds that takedown of the content was unduly restrictive of free speech and it was technically not feasible to delete content that was republished multiple times on different platforms.

You are a Justice of the High Court of Nyaya Pradesh, submit your reasoned opinion in reference to relevant provisions and case laws.

(Marks 20)

Q 3) Kindly read the following fact situations carefully:

**(a)** The Municipal Corporation of Pune collected medical records of children suffering from visual impairment in order to distribute assistive educational devices. The data was collected with verifiable parental consent. The Corporation later shared the data with a government hospital in Mumbai for the purpose of providing these children subsidized eye check-ups, without obtaining fresh consent.

**(b)** A group of doctors at a government medical college in Chennai conducted research on HIV transmission patterns. They published the results of the study in a reputed medical journal published online and offline. They included the names and test results of HIV-positive patients without obtaining prior consent for such publication.

**(c)** A mobile application used by adults across Delhi NCR for news aggregation and lifestyle content tracks how users use their app, including what they click on, how long they stay on articles, and their interactions. The users have not been explicitly informed consequently nor do they have the option to opt in or opt out of such tracking.

**(d)** A man suffered a severe road accident while travelling from Bhubaneswar to Cuttack and was admitted to a hospital in an unconscious state. The hospital accessed and processed his personal and health records from his primary care provider.

Assume that the Digital Personal Data Protection Act, 2023 (DPDPA) is fully in force in India. Analyze the validity of personal data processing in these four independent fact situations. You must clearly state whether the processing is lawful, and if not, why, referring to relevant provisions.

(Marks 5 x 4 = 20)

Q 4) Write short notes on the following topics –

a) Data Portability
b) Data Protection Impact Assessment

(Marks 10 x 2 = 20)

Q 5) The principle of Data Protection by Design and by Default places a proactive responsibility on data fiduciaries to embed privacy and data protection measures into the design and functioning of systems and processes that involve the processing of personal data.

Critically examine the scope and significance of this principle under the EU GDPR, particularly:

a) The meaning and objectives of Data Protection by Design and Data Protection by Default.
b) The extent to which this principle is reflected in the obligations of data controllers under the EU GDPR.
c) The relevance of this principle in the context of automated decision-making, behavioural profiling, and children's data.
d) A comparative reference to how this principle is reflected under the DPDPA 2023.

(Marks 5 x 4 = 20)

Q 6) Priyansha is an avid user of FaceGram, a popular social media platform with millions of users worldwide. She has been active on the platform for over five years, during which time she has uploaded personal photographs, shared location data, reacted to posts, interacted with targeted advertisements, and participated in various quizzes and surveys promoted by third-party apps through the platform.

Recently, Priyansha grew concerned about how much of her data was being used to profile her for behavioural targeting and advertising. Over a span of two months, she submitted four separate data access requests to FaceGram, asking for:

- A copy of all personal data collected and processed about her;
- Information about profiling and automated decision-making based on her behaviour;
- A list of third parties and advertisers with whom her data was shared;
- The logic behind targeted content and advertisements shown to her.

In response, FaceGram denied her most recent request, stating that her "repetitive and excessive" use of the right to access imposes an unreasonable burden on the platform. The company further stated that it had already responded in part to a previous request, and its systems were not equipped to handle such granular or frequent disclosures on an ongoing basis. Priyansha believes this is an unjustified denial of her fundamental right and is considering legal action.

a) If Priyansha is an Indian citizen, advise her on her rights under the Digital Personal Data Protection Act, 2023, the obligations of the data fiduciary (FaceGram), and

whether this denial of access may be valid in light of the provisions of the Act. What remedies can she pursue, and through what mechanism?

b) If Priyansha is a French citizen, advise her on her rights under the EU General Data Protection Regulation (GDPR). Assess whether FaceGram's refusal aligns with GDPR provisions, and outline the steps she may take, including lodging complaints with supervisory authorities or seeking judicial remedies.

In both cases, refer to the scope of the right to access, possible limitations or exemptions, and the role of regulatory authorities in enforcing data subject rights.

(Marks 10 x 2 = 20)