



# DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to Visvesvaraya Technological University (VTU), Belagavi,  
Approved by AICTE and UGC, Accredited by NAAC with 'A' grade & ISO 9001-2015 Certified Institution)

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru - 560 111. India

DEPARTMENT	ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING				
Semester: VII	Course Title: Data Security & Privacy Lab			Course Code: 22AI73	
PROGRAM QUESTION	10) Case Study on GDPR and DPDP Act 2023: create a comparative chart of GDPR and DPDP Act 2023 principles and explain roles like Data Protection Officer (DPO). Include a mock incident report format.				
STUDENT NAMES	SURYANSHU DHARGAVE	USN	1DS22AI055		
LAB MARKS	Program Execution (10)	Source Code (10)	Result (5)	Innovation/ Extra Features (5)	Total
TOOLS USED	VS Code				
MAP COURSE OUTCOME	CO2				
MAP PROGRAM OUTCOME	PO1, PO2, PO6, PO7, PO8				
MAP PROGRAM SPECIFIC OUTCOME	PSO1, PSO2				
UML / SEQUENCE DIGRAM	<div><div>Identify Data Breach</div><div>Notify DPO</div><div>Report to Authority</div><div>Document Incident</div></div> <div><div>INCIDENT REPORT</div><div>Incident Date:</div><div>Description of Incident:</div><div>Data Involved:</div><div>Impact:</div><div></div></div>				
COURSE COORDINATOR	Dr ARUNA M G & Prof ENSTEIH SILVIA				

## Program 10:

### Introduction

Data privacy has become a critical issue in the digital era. The **European Union's General Data Protection Regulation (GDPR)** and **India's Digital Personal Data Protection (DPDP) Act, 2023** are both designed to safeguard individuals' personal data, but they differ in scope, enforcement, and legal structure.

### GDPR vs DPDP Act 2023 Comparison

Aspect	GDPR (EU)	DPDP Act 2023 (India)
Full Form	General Data Protection Regulation	Digital Personal Data Protection Act, 2023
Effective From	May 25, 2018	August 11, 2023
Governing Authority	European Data Protection Board (EDPB) and National Supervisory Authorities	Data Protection Board of India
Scope	Applies to processing of data of EU citizens, even by foreign entities	Applies to digital personal data of Indian citizens, processed within or outside India (if offering goods/services in India)
Applicability	Both digital and manual (paper-based) data	Only digital personal data
Definition of Personal Data	Any information relating to an identified or identifiable natural person	Any data about an individual who can be identified by such data
Sensitive Data	Special categories like health, biometric, racial origin, religion, etc.	Sensitive data categories not explicitly defined (may be notified later)
Consent	Must be freely given, specific, informed, and unambiguous	Must be free, specific, informed, unconditional, and unambiguous with clear affirmative action
Data Principal / Subject Rights	Right to access, rectification, erasure, restriction, portability, and objection	Right to access, correction, erasure, grievance redressal, and nominate a representative in case of death/incapacity
Children's Data Protection	Parental consent required below age 16 (member states can lower to 13)	Parental consent required below age 18
Cross-Border Data Transfer	Permitted to countries with adequate protection	Permitted to countries notified by the Central Government
Penalties	Up to €20 million or 4% of global annual turnover (whichever higher)	Up to ₹250 crore per instance of non-compliance
Data Breach Notification	Must notify authority within 72 hours	Must notify Data Protection Board and affected users (timeline not specified)
Right to Be Forgotten	Explicitly mentioned	Provided under Right to Erasure
Data Protection Officer (DPO)	Mandatory for large-scale or sensitive data processing organizations	Required for significant data fiduciaries as notified by the government
Enforcement Mechanism	Independent supervisory authorities	Data Protection Board of India with adjudicatory powers
Exemptions	National security, defense, law enforcement	National security, research, government functions, or legal compliance
Incident Management	Notify supervisory authority + affected individuals; keep records of incidents	Notify Data Protection Board + affected users; maintain incident records

## Role of Data Protection Officer (DPO)

Aspect	GDPR	DPDP Act 2023
<b>Appointment</b>	Mandatory for public authorities, organizations engaged in large-scale systematic monitoring, or processing sensitive data.	Required for “Significant Data Fiduciaries” as notified by the Central Government.
<b>Reporting Authority</b>	Reports directly to top management.	Reports to the Board of Directors or equivalent authority.
<b>Responsibilities</b>	- Monitor compliance with GDPR- Conduct data protection impact assessments- Serve as contact point for data subjects and supervisory authorities- Advise on data protection obligations	- Ensure compliance with DPDP Act- Coordinate with the Data Protection Board of India- Handle grievances and data principal requests
<b>Qualification</b>	Expertise in data protection laws and practices	Professional with knowledge of privacy and data protection practices
<b>Independence</b>	Must act independently without conflict of interest	Expected to act neutrally and protect user data as per the Act