Assignment-1

1) Describe the technical measures and safeguards that organizations can implement to ensure compliance with the GDPR's data protection principles.

→ IDAM - Identity and access management
Help limit access to personal data for authorized employees. Have access only to information or systems applicable to their job.

→ DLP - Data Loss prevention.
prevents the loss of personal data.

→ Encryption - processing of personal data in such a way that data can no longer be attributed to a specific data subject.

→ IRP - Incident Response plan
Process of preparation, identification, eradication, containment, recovery and lessons learnt.

2) Concept of Privacy by design and default as mandated by GDPR.

It means data protection through tech. design. Behind this is thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created.

3) Role of cryptographic techniques in ensuring data security and compliance with data.

→ Data encryption
→ Access control
→ Auditing and logging
→ Data Integrity
→ Secure data storage
→ Secure comms.

5) The technical implications of complying with California Consumer privacy act.

The CCPA provides its Cali citizens with a higher degree of control over their online personal information by providing rights over their online personal data and how companies use it. # outlines certain restrictions and exemptions to specific data categories.

6) Implementing a robust Access control mechanism to comply with data protection regulations.

-> Understanding the DPDA

-> Data Cover

-> Information Lifecycle management

-> Data life cycle management

7) Distributed ledger Technologies such as blockchain impact compliance with data protection regulations like GDPR and CCPA?

The BCT framework makes data stored on network visible to those with access, making it challenging to comply with GDPR's data privacy and protection requirements.

Unless the personal data stored on the block chain is truly anonymised the storage and processing of data will need to comply with EU regulations.

8)

→ Define what to forget
→ Survey business intelligence systems
→ Don't forget the emails
→ educate employees about shadow data
→ Data governance

9)

Protecting an IOT network includes ensuring port security, disabling port forwading and never opening ports when not needed, using anti malware, firewalls, intrusion detection systems and intrusion prevention systems. blocking unauthorized IP addresses.

10)

→ Transparency and information requirements for online-services.

→ commercial communications

→ electronic contracts and limitations of liability of intermediary service providers.

→ Internal market clause

→ liability of intermediaries