GDPR에 따른 데이터 암호화 방식

1. **전송 중 암호화**
    - 데이터를 전송하는 동안 보호하는 방식, 서버 간 이동 시 해커가 데이터를 탈취하지 못하도록 함
        - TLS (Transport Layer Security): HTTPS 프로토콜을 통해 데이터를 보호하며, SSL (Secure Sockets Layer) 의 후속 기술
2. **저장 중 암호화**
    - 데이터가 저장될 때 적용하는 암호화 방식, 데이터 베이스나 파일 시스템에 저장된 데이터를 보호
        - AES (Advanced Encryption Standard): 대칭 키 암호화 방식으로, 금융과 정부 기관에서 널리 사용됨
        - RSA (Rivest-Shamir-Adleman): 공개 키 암호화 방식으로, 개인 키와 공개 키를 사용하여 데이터를 안전하게 보호
3. **암호화 키 관리**
    - GDPR 에서는 키 관리 정책의 중요성을 강조함. 키가 무단으로 노출되거나 분실될 경우 데이터가 탈취될 수 있기 때문에
        - HSM (Hardward Security Module): 암호화 키를 보호하기 위해 물리적 장비에 키를 저장하고 관리하는 방식
        - KMS (Key Management Service): 클라우스 제공자가 제공하는 암호화 키 관리 서비스

GDPR에 따른 데이터 암호화 방식