국가 간 데이터 이전의 주의사항

3. 데이터 거버넌스와 권할권 문제

- 어떤 국가에 저장된 데이터가 다른 국가 법률의 적용을 받는지에 대한 문제가 발생할 수 있음
- 데이터가 미국에 저장되면 미국 법률의 영향을 받을 수 있으며 이 경우 개인 정보 보호가 제3국의 요구에 의해 위협 받을 가능성도 있음
- 이로 인해 기업은 데이터가 저장된 위치와 해당 국가의 법률이 어떻게 적용되는 지에 대한 명확한 이해와 관리 필요

4. 데이터 로컬화 요구사항

- 일부 국가는 자국민의 개인 정보를 국가 내부에 저장할 것을 요구하는 **"데이터 로컬화"** 규제가 있음
- 일본은 엄격한 규제는 없지만 **APPI**에 따른 절차를 준수해야 함
- 중국, 러시아, 인도 등은 자국의 데이터가 해외로 이전되지 않도록 요구하는 규제 존재
- 이는 데이터 이동을 제한할 수 있고 기업이 현지에 데이터 센터를 구축해야하는 부담이 초래 됨

* **APPI**: Act on the Protection of Personal Information 으로 일본의 개인 정보 보호법. 외국 기업이 일본 내에서 따라야 할 표준을 명확히 규정하고 있음

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