GDPR(General Data Protection Regulation)

1. GDPR 이란?

> GDPR은 유럽연합 일반 개인정보 보호법'General Data Protection Regulation'의 약자로 EU 거주자의 개인 정보를 강화하고 표준화하기 위해 제정되었습니다. 이는 기존에 EU 개인 정보 보호 기준을 제시하였던 '1995년 개인 정보보호 지침' 을 대체하는 법적 구속력을 가진 규정으로 올해 5월 25일부터 시행되었습니다.

GDPR의 주요변화 항목

ㅇ개인에 대한 권리 확대

유럽 연합 내 개인에게 잊힐 권리와 저장된 개인 데이터의 사본을 요구할 권리를 부여함으로써 확대된 권리를 제공합니다. 또한 조직은 정보 주체로 부터 개인 정보 사용에 대해 간결명료하게 설명하여 이에 동의를 얻어야 합니다.

ㅇ데이터 유출 알람 및 보안

조직은 개인 정보 보안에 위협이 될 만한 모든 침해 사실에 대해 정보 주체에 공지할 의무가 있습니다.

ㅇ개인 정보 수집 및 모니터링에 대한 추가 적인 의무 조치 사항(ex: cctv)

EU개인의 행동을 수집하거나 모니터링하는 조직에 대해 개인 정보 침해를 막기 위한 정책이나 기술적 제어 등 정보처리에 대해 추가적인 보안적 초치사항을 요구합니다.

ㅇ정보 보호 책임자(DPO)지정

데이터 보호 책임자(Data Protection Offcer)는 공공 기관 또는 정보주체에 대한 "대규모의 정기적이고 체계적인 모니터링"에 종사하는 기관이거나 민감한 개인 데이터나 범죄 경력 및 범죄 행위에 대해 "대규모"로 처리하는 기관의 경우 필수적으로 지정해야합니다.

ㅇ집행 강화.(과징금 확대)

2. 뽕카와 IMS에 미치는 영향

이 규정은 EU 내에서 사업장을 운영하며 개인 정보를 다루는 기업과 EU 외에서 EU 거주자에게 재화나 서비스를 제공하는 기업. 즉, EU 내에 사업장을 가지고 있지 않더라도 EU 거주자를 대상으로 개인 정보를 수집하고 처리하는 경우에 의무 대상에 해당됩니다.

위 규정에 의하면 뽕카와 IMS는 웹 서비스로서 EU 거주자가 해당 서비스를 이용할때 GDPR 적용이 가능해 보이지만 지난 해 11월 벨기에 브뤼셀에서 개최된 '한·EU 기업간담회'에서 나온 질의·응답에 의하면 'GDPR의 적용범위'는 정보주체의 '국적' 이 아닌 '위치'가 기준이기 때문에 국내에서만 서비스하는 뽕카와 IMS에 미치는 영향은 무관하다고 생각됩니다.

3. 영향이 있다면 대응방안

- 사용할 개인 정보에 대한 동의(및 철회)방법을 모두 문서화 하고 분명하고 쉽게 만든다.
- 데이터 침해의 영향을 받은 사람에게 72시간 이내에 관련 정보를 알린다.
- 소비자들이 기업이 자신의 어떤 개인 정보를 다루고 있는지 알 수 있도록 한다.
- 소비자가 정보 삭제와 제3자에 대한 정보 공유 중단을 요청할 때 이에 대한 조치를 취한다.

- 개인 정보를 저장하고 처리하는 시스템의 보안을 유지한다.
- 위의 모든 조치가 실시되는지의 여부를 확인하기 위한 분명한 검증 절차를 갖춘다.

4. GDPR에 대한 보안정책

Quik(기업용 SNS): https://www.quik.co.kr/security

ㅇ 사용자 인증

사용자가 로그온 할때마다 사용자 고유 이름(이메일주소)과 비밀번호를 요구 합니다. 사용자 고유 이름과 비밀번호를 통하여 사용자 인증을 거치며, 인증정보는 세션을 통해 안전하게 관리합니다.

ㅇ 비밀번호 암호화

가입된 사용자들의 비밀번호는 완전하게 암호화되어 데이터베이스에 저장됩니다. 복호화가 불가능하게 암호화하여 저장하므로, 시스템관리자도 사용 자의 비밀번호를 알 수 없습니다.