유럽 개인정보보호법(General Data Protection Regulation, GDPR)이 2018 년 5 월부터 시행됩니다.

유럽에서 사업을 하거나 유럽 시민을 고용하는 등

유럽시민의 개인정보를 사용하고자 하는 기업/기관은 반드시 GDPR 에 대응해야만 하는데요,

시행 이후 유럽시민의 개인정보를 잘못 취급할 경우

천문학적인 벌금을 물기 때문에 유럽과 관련된 우리나라 기업들은 반드시 이 제도를 준수해야만 합니다.

하지만 복잡하고 애매모호한 GDPR 때문에

기업들은 이를 준수하기 위한 시스템 및 절차를 준비하는 과정에서 어려움을 겪을 것으로 예상됩니다.

유럽 개인정보보호법, GDPR

▲ GDPR 정의

유럽 의회에서 유럽 시민들의 개인정보 보호를 강화하기 위해 만든 통합 규정으로 2016 년 유럽 의회에서 공표되었으며(Regulation(EU) 2016/679), 약 2 년간의 유예 기간을 갖은 후 2018 년 5 월 25 일부터 EU 각 회원국에서 시행된다.

유럽 연합의 시민의 데이터를 활용하는 경우 GDPR 을 준수해야 하는데 GDPR 의 주요 항목은 사용자가 본인의 데이터 처리 관련 사항을 제공 받을 권리, 열람 요청 권리, 정정 요청 권리, 삭제 요청 권리, 처리 제한 요청 권리, 데이터 이동 권리, 처리 거부 요청 권리, 개인정보의 자동 프로파일링 및 활용에 대한 결정 권리 등이다.

출처 : 네이버 지식백과

이미 유럽연합에서는 1995 년부터 개인정보 보호를 위한

EU 개인정보보호지침(Directive 95/46/EC)를 시행하고 있었는데요

1 년 전인 2016 년 4 월 이 지침을 대체하는 GDPR 이 유럽의회로부터 승인되어

구시대의 정보보호명령을 대체했습니다.

GDPR 조항에 따라 기업들은 EU 회원국 내 발생하는 거래에 대해

EU 시민의 개인/사생활 정보를 보호하는 것을 의무화 해야 하며 EU 외부로의 개인정보 유출도 규제됩니다.

GDPR 조항은 EU 전체 회원국 28 개국에 동일하게 적용되는데요

조항들이 상당히 까다롭기 때문에 이를 충족하고 관리하려면

대부분의 기업에서 대규모의 투자가 필요할 것으로 예상됩니다.

▲ GDPR 적용 대상

- EU 국가에 사업장을 보유한 경우

- EU 에 사업장은 없으나 유럽 거주자의 개인 정보를 처리하는 경우

- 직원 수가 250 명 이상인 경우

- 직원 수는 250 명 미만이지만 정보 처리를 통해 정보 주체의 권리와 자유에 영향을 미치고, 정보 처리가 드물지 않게 일어나거나 특정 종류의 민감한 개인 정보를 처리하는 경우

EU 국가 내에서 EU 시민에 관한 개인 정보를 저장하거나 처리하는 기업이라면

모두 GDPR 준수 의무화 대상인데요

EU 에 사업장을 가지고 있지 않더라도 EU 거주시민을 대상으로

재화와 서비스를 제공하기 위해 개인정보를 수집하는 경우도 적용됩니다.

▲ GDPR 가 적용되는 개인정보 범위

- 이름, 주소 ID 등 기본 신상 정보

- 위치 IP 주소, 쿠키, 데이터, RFID 태그 등 웹 정보

- 건강, 유전 정보

- 생체 정보

- 인종 또는 민족 정보

- 정치적 의견

- 성적 취향

GDPR 이 적용되는 개인정보 범위는 식별 가능한 자연인 정보에

이름, 위치정보와 같은 식별자와 함께 온라인 식별자 정보, 유전자 정보 등도 포함 됩니다.

온라인 식별자 정보는 IP, Mac Address, cookies, 시리얼 넘버 등을 꼽을 수 있습니다.

▲ GDPR 위반 시 처벌

- 개인정보 처리 원칙, 동의요건, 국외이전 등 심각한 위반 시 전세계 연간 매출액의 4% 또는 2 천만 유로 중 높은 금액 이, 그 외의 일반적 위반의 경우 전세계 연간 매출액의 2% 또는 2 천만 유로 중 높은 금액이 과징금으로 부과될 수 있다.

- 과징금 부과 여부 및 금액에 대한 결정은 회원국 감독기구에 있다.

GDPR 을 반드시 준수해야 하는 가장 큰 이유이지요.

GDPR 규정 불이행 시 엄청난 벌금을 물도록 규정하고 있는데요,

위반 시 최대 2000 만유로(약 260 억원) 혹은 전 세계 매출의 4% 중 더 큰 금액이 과징금으로 부과됩니다.

예로 들어 한 해 200 조원의 매출을 올리는 기업일 경우 과징금이 무려 8 조에 이르는 셈인데요,

일반적 위반의 경우라 해도 1000 만유로 혹은 전 세계 연간 매출액의 2% 중

더 높은 금액이 부과돼 심각한 비즈니스 피해를 입을 수 있습니다.

다가오고 있는 GDPR, 국내외 기업들은 어떻게?

위의 내용과 같이 유럽 개인정보보호 규정이 전 산업계 위험요소로 부상하고 있지만

국내외 산업계에선 심각성을 크게 인식하지 못하고 있어 우려가 되는 상황입니다.

국내의 경우 일부 대기업을 제외하곤 대응을 준비하지 않고 있는데요

올해 2~3 월 EU 와 거래 중인 기업 관계자 100 명을 대상으로 실시한 설문조사 결과,

61%의 기업인이 내년 5 월 내 GDPR 대비를 못 마칠 것이라고 응답했으며

무려 40%의 기업인은 내부에 실시한 DB 관리도구가 없어서 DB 관리가 불가능한 상태라고 밝힐 정도로

대부분의 기업에서 자체 대응은 커녕 정보파악도 제대로 하지 않고 있는 것으로 파악되었습니다.

이러한 상황은 해외도 마찬가지인데요,

NTT 시큐리티가 7 월 발표한 보고서에 따르면

글로벌 기업 임원 20%는 GDPR 이 비즈니스에 어떤 영향을 미칠지 인지하지 못하는 것으로 나타났습니다.

GDPR 규제 발효 후 기업이 보유한 EU 회원국 국민의 개인정보가 침해될 경우

해당 기업은 바로 GDPR 을 위반한 것으로

제대로 대응하지 못하면 그 피해를 기업이 고스란히 지기 때문에 철저하게 대비를 해야 합니다.

GDPR 대응 방안

▲ 사내 규정 준수 담당자 고용 또는 임명

GDPR 에 규정된 규정 준수 담당자는 크게 정보 통제자, 정보 처리자, 정보 보호 책임자(DPO) 입니다.

정보 통제자는 개인 정보 처리 방식과 목적을 정하고 외부 계약 업체의 규정 준수도 책임지는 역할을 맡고 있습니다.

정보 처리자는 개인 정보 기록 유지 관리와 처리를 담당하며

내부에서 그룹을 지정할 수 있고 이런 활동을 전부 또는 일부를 수행하는 외주 업체를 지정할 수 있습니다.

GDPR 은 규정 위반이나 불이행의 책임을 정보 처리자에게 묻는데

해당 기업은 물론 클라우드 제공업체와 같은 정보 처리 협력업체 역시

불이익에 대한 책임을 져야 할 가능성이 있습니다.

마지막으로 정보 보안 전략과 GDPR 준수를 감독한 데이터 보호 담당자(Data Protection Officer , DPO)를

정보 통제자와 정보 처리자가 지명해야 합니다.

DPO 의무화 대상은 많은 양의 EU 시민 정보를 처리하거나 저장하는 기업,

특수 개인정보를 처리하거나 저장하는 기업, 정보 주체를 주기적으로 감시하는 기업이며

공공 기관도 의무화 대상입니다.

▲ GDPR 요건과 일치한 정보 보호 계획 수립

이미 계획이 수립되어 있더라도 재검토하여 GDPR 요건과 일치하도록 업데이트 해야 합니다.

▲ 위험 경감 조치 이행

위험과 그 경감 방법을 파악하면 위험 경감 조치를 시행해야 합니다.

대부분의 회사에서 이는 기존 위험 경감 조치를 수정하는 것을 의미합니다.

▲ 사고 대응 계획 테스트

GDPR 은 정보 침해 시 기업들이 72 시간 이내에 신고할 것을 의무화 하고 있습니다.

기업이 규정 위반으로 벌금을 물 것이냐는 대응팀이 얼마나 효과적으로 피해를 최소화 하느냐에

직접적으로 좌우되므로 기한 내에 적절한 신고와 대응이 가능하도록 조치해야 합니다.

▲ 지속적 평가를 위한 절차 수립

규정은 계속 준수해야 하며 이를 위해서는 감시와 지속적인 개선이 필요합니다.