EU GDPR 이해하기

행정안전부

유럽 개인정보보호법
General Data Protection Regulation

GDPR이란?

2018년 5월 25일부터 시행되는 EU(유럽연합)의 개인정보보호 법령이며, 동 법령 위반시 과징금 등 행정처분이 부과될 수 있어 EU와 거래하는 우리나라 기업도 이 법에 위반되지 않도록 주의할 필요가 있습니다.

GDPR 시행에 따른 주요 변화

구분	Before (Directive 95/46/EC)	After (GDPR)
기업의 책임 강화	개인정보 최소 처리, 처리목적 통지 등	**개인정보보호책임자 지정, 영향평가 등 추가**
정보주체 권리 강화	열람 청구권 등	**정보이동권 등 새로운 권리 추가**
과징금 부과	회원국별 자체 법규에 따라 부과	**모든 회원국이 통일된 기준으로 부과**

GDPR을 적용받는 기업은?

아래 어느 하나에 해당하는 기업으로서 EU 주민의 개인정보를 처리하는 경우에는 한국 기업도 적용 대상임

- EU에 사업장을 운영하는 기업(지점, 판매소, 영업소 등)
- EU 지역에 사업장은 없지만, 인터넷 홈페이지를 통해 EU에 거주하는 주민에게 물품·서비스를 제공하는 기업
  - (예) 현지어로 마케팅 활동을 하거나 현지 통화로 결제하는 경우
- EU 주민의 행동을 모니터 하는 기업

특히 아래에 해당하는 기업은 특별한 주의를 요함

- EU 주민의 민감한 정보(건강, 유전자, 범죄경력 등)를 처리하거나, 아동의 정보를 처리하는 기업
- 공개적으로 접근 가능한 장소에 대한 대규모의 체계적인 모니터링을 하는 기업(예 : CCTV)

GDPR에 따른 기업의 책임 강화

- 전문지식을 갖춘 개인정보보호책임자(DPO, Data Protection Officer)지정
- 민감한 정보를 대규모로 처리하는 기업 등의 경우에는 개인정보 영향평가 실시
- GDPR을 준수하고 있음을 입증하기 위해 개인정보 처리활동에 관한 기록 유지
- EU 외 지역에서 EU 주민의 개인정보를 대규모로 처리하는 경우에는 EU 역내에 대리인을 지정해야 함
- 해킹 등 유출사고 발생시 감독기구에 신고하고 중대한 위험 가능성이 있는 경우에는 정보주체에게 통지
- 정기적 검사 및 평가 등 적절한 기술 및 관리 조치 이행
- 정보주체의 권리 보장을 위한 절차 마련·이행

<참고 : GDPR에서 신설·강화된 정보주체의 권리>

권리	주요내용
처리제한권(신설)	정보주체는 본인에 관한 개인정보의 처리를 차단하거나 제한을 요구할 권리를 가짐
정보이동권(신설)	정보주체는 본인의 개인정보를 본인 또는 다른 사업자에게 전송토록 요구할 권리를 가짐
삭제권(강화)	정보주체는 본인에 관한 개인정보 삭제를 요구할 권리를 가짐
프로파일링 거부권(강화)	정보주체는 본인에게 중대한 영향을 미치는 사안에 대해 프로파일링 등 자동화된 처리에 의한 결정을 반대할 권리를 가짐

개인정보 국외 이전 방안

- **개별 기업이 EU 주민 개인정보를 한국으로 가져오는 방법**

구분	주요내용
표준개인정보 보호 조항	EU 집행위가 승인한 표준 조항이 반영된 계약을 통해 개인정보를 이전하는 경우
의무적 기업규칙	EU 회원국 감독당국이 승인한 구속력이 있는 의무적 기업규칙에 따라 이전하는 경우
행동강령	EU 집행위가 승인한 행동강령에 따른 이전
인증	EU 회원국 정보보호 인증을 받은 자에게 이전
기타	정보주체의 명시적 동의, 중요한 공익상 이유 등

- **개인정보 보호 수준이 EU와 동등하다고 인정될 경우(적정성 평가) 위의 조치 없이 이전 가능**
  현재 온라인 분야에 대해 정보통신망법을 중심으로 한국과 EU가 일괄 협의 중

우리나라 기업은 무엇을 준비해야 하나?

- **경영진의 인식 제고**
  주요 의사 결정권자 등의 인식제고와 예산, 인력 등을 포함한 전사적 대응방안을 준비
- **개인정보보호책임자(DPO) 지정**
  전문적 지식과 실무 경험이 있는 전문가를 지정
- **개인정보보호 계획 수립**
  조직 내 개인정보 처리 현황 등을 점검하고 GDPR 요구 내용을 충실히 반영한 내부 계획을 수립·운영(정보주체 권리보장 절차 등)
- **자체 점검 및 개선 조치**
  보관 중인 개인정보의 항목, 처리 방법의 적법성, 동의 획득 절차, 대리인 지정, 국외 이전 발생 여부 등을 면밀히 점검하고, 법 위반 우려가 있는 경우에는 신속히 개선 조치

법 위반시 과징금 수준은?

일반적 위반 사항 (대리인 미지정 위반 등)	중요한 위반 사항 (국외 이전 규정 위반 등)
전 세계 매출액 2% 또는 1천만 유로(약 125억원) 중 높은 금액	전 세계 매출액 4% 또는 2천만 유로 (약 250억원) 중 높은 금액

- 위 과징금은 최대 한도의 부과 금액을 말하여 실제 부과 금액은 위반 내용, 피해경감 노력 등 11개 기준을 종합 검토하여 결정됨
- 구체적 과징금 부과 요건 및 집행절차 등은 EU 회원국 현지의 법률 제·개정 동향 및 판례 등을 지속 모니터할 필요가 있음

GDPR 관련 주요 질의 응답 사례

Q1. GDPR의 영향을 받는 기업은?

- 국내에서만 영업을 하는 기업에는 아무런 영향이 없고 EU에 현지 영업소를 두거나 EU 주민을 대상으로 영업을 하는 기업은 GDPR 준수를 위한 준비가 필요함

Q2. 기업이 무엇을 어떻게 준비해야 하나?

- **(1단계)** 해당 기업 내 개인정보 처리 현황 등을 점검하여 GDPR 적용 대상인지 확인
- **(2단계)** GDPR 적용 대상인 경우 기 배포된 안내서 및 가이드라인 등을 참고하여 개인정보보호책임자(DPO) 지정 등 즉시 조치 가능한 사항을 시행해야 함
- **(3단계)** 개인정보 처리 방법의 적절성, 동의 획득 절차, 국외 이전 여부, 대리인 지정 필요성 등을 점검하여 법 위반 우려가 있는 사항은 신속히 개선 조치

※ 'EU GDPR 대비 기업이 준비해야 할 사항' 참조(한국인터넷진흥원 자료실)

Q3. 이전 EU 지침과 비교시 GDPR 시행으로 달라지는 점?

- 이전 EU 지침은 권고 차원의 규정인 점에 반해, GDPR은 모든 회원국 등이 의무적으로 준수해야하는 강행 규정이라는 점에서 큰 차이가 있음(위반시 과징금 부과)
- 아울러, GDPR은 개인정보보호책임자(DPO) 지정, 개인정보 처리활동의 기록 · 유지, 개인정보 영향평가 실시, 역내 대리인 지정 등 기업의 책임성을 강화하는 내용과 처리제한권, 정보이동권 등 정보주체 권리를 신설하는 내용이 추가되었음

Q4. 개인정보보호책임자(DPO, Data Protection Officer)란 무엇이며 어떤 경우 지정해야 하나요?

- DPO란 개인정보보호 관련 전문지식을 갖추고 기업 내 조언자이자 감독자 역할을 수행하는 사람임

※우리나라의 임원급 개인정보보호책임자(CPO, Chief Privacy Officer) 지정 제도와 유사하며, 다만 전문지식에 대한 보완 필요

- 특히 ① 개인정보를 처리하는 공공기관, ② 정보주체에 대한 정기적이고 체계적인 모니터링을 하는 경우, ③ 건강정보, 범죄경력 등의 민감한 정보를 처리하는 기업의 경우에는 필수적으로 지정해야 함

Q5. 개인정보의 이동을 요구할 권리란 무엇인가요?

- 정보주체가 자신이 A기업에게 제공했던 개인정보를 체계적 형태(CSV, XML 등)로 다시 전달 받거나 그 개인정보를 다른 B기업으로 이전할 것을 요구할 수 있는 권리임

* (예) 이메일 업체 변경시 기존 등록된 연락처를 변경한 업체로 이동

- 다만, 이전을 요구할 수 있는 정보에는 추론(inferred) 또는 파생(derived)을 통해 A기업이 생성한 정보는 포함되지 않음.

Q6. EU 지역 주민의 개인정보를 우리나라로 이전할 수 있는 방법은 무엇인가요 ?

- EU에서 인정한 적절한 보호조치가 있는 경우 이전 가능

* 예를 들어 개별 기업 차원의 표준계약 체결, 구속력있는 기업규칙(BCR), 공인 행동강령 또는 개인정보보호인증 등의 방법이 있음.

- 또한, 개인정보 보호 수준이 EU와 동등하다고 인정되는 국가에는 위의 절차를 거치지 않고도 개인정보 국외 이전이 가능하며, 이에 대하여는 현재 한국과 EU간 온라인 분야의 일괄 협의가 진행 중임(적정성 평가)

Q7. 위반시 막대한 과징금이 부과된다고 하는데?

- GDPR에 규정된 과징금 액수는 최대 한도의 과징금을 말하며, 실제 부과 금액은 위반의 내용, 의도성, 피해경감 노력 등 11개 기준을 종합 검토하여 결정됨
- 다만, 1회 위반하였다 하여 과징금이 바로 부과되는 것이 아니라 시정요구 등의 여러 절차를 거쳐야 하므로 기업 책임사항을 내실있게 준비하여 피해를 미리 예방할 필요

Q8. 기타 유의해야 할 사항은 무엇인지?

- 과징금 부과대상에 해당하지 않는 GDPR 위반사항에 대하여도 각 회원국은 자국의 법률에 추가적인 처벌(징계 등)을 규정할 수 있음
- 따라서, 특정 국가에서 사업을 영위하는 경우에는 해당 국가의 법률을 지속적으로 모니터링 해야 함

※ EU에 사업장을 운영하는 기업은 현지 법률 컨설팅 활용 권고

기타 안내사항

상담문의처

- 대한무역협회(02-6000-4245)
- KOTRA(02-3460-7593)
- 한국상장사협의회(02-3275-3094)
- 대한상공회의소(02-6050-1509)
- 중소기업중앙회(02-2124-3163)
- 한국화학융합시험연구원(02-2164-1421)
- 한국인터넷진흥원(061-820-1805)

인터넷 자료실

- 한국인터넷진흥원 GDPR 자료실(http://gdpr.kisa.or.kr)
- 개인정보보호위원회 EU GDPR 자료실(http://www.pipc.go.kr)
- EU 집행위원회 홈페이지(http://www.eugdpr.org)