

■ 칼럼 ■

EU 개인정보보호법(GDPR) 시행이 국내 기업에 미치는 영향

(법무법인(유) 지평 [이해원 변호사](#))

2018년 5월 25일부터 유럽연합(EU)의 개인정보보호법(General Data Protection Regulation, 약칭 'GDPR')이 EU 28개 전 회원국에서 시행됩니다. GDPR은 개인의 존엄성(dignity)을 존중하는 유럽의 전통과 철학을 충실히 반영하여 개인정보를 두텁게 보호하고 이를 위반한 기업에게는 최대 전 세계 매출액의 4% 또는 2천만 유로(약 250억 원)의 과징금을 부과할 수 있도록 제재 규정을 대폭 강화하였습니다.

GDPR의 가장 큰 특징은 EU 회원국 내 거주자에게 재화와 서비스를 제공하거나 EU 회원국 내 거주자의 EU 내에서의 행동을 모니터링 하는 기업이라면 국적에 상관없이 GDPR을 적용하는, 소위 '역외 적용'(extraterritorial application) 조항을 두고 있다는 점입니다. 우리나라 기업이라도 EU 회원국 내 거주자를 상대로 물품을 판매하거나 서비스를 제공하고 있다면, GDPR에 따라 개인정보보호에 필요한 각종 조치를 취해야 하며, 그렇지 않을 경우 고액의 과징금을 물게 될 위험이 있습니다. 예를 들어 우리나라 기업이 웹사이트나 모바일 앱 등을 통하여 EU 회원국의 언어(영어, 프랑스어, 독일어 등)와 EU의 통화(유로, 파운드 등)를 지원하고 EU 회원국에 상품을 배송하는 국제 배송 서비스를 제공하는 경우 '역외적용' 조항에 따라 GDPR의 적용을 받게 될 가능성이 매우 높습니다.

GDPR의 역외적용 대상 기업은 GDPR의 규정에 따라 개인정보를 처리해야 하고, GDPR에서 규정한 정보주체의 권리를 보장해야 하며, EU 회원국 내에 대리인(representative)를 지정해야 하고 EU 개인정보보호 당국의 감독을 받아야 하는 등 추가적인 자원과 비용을 투입해야 하는 부담이 있습니다. 특히 GDPR은 기존의 유럽개인정보보호지침(Directive 95/46/EC)보다 개인정보보호를 강화하여 개인정보 이동권(Right to data portability), 자동화된 결정 및 프로파일 관련 권리(Right to related to

automated decision making and profiling)와 같은 정보주체의 새로운 권리를 도입하고, 개인정보의 처리를 위하여 해당 정보주체의 '유효한 동의'를 받도록 규정하며, 이용 약관 등에 동의하는 정도로 유효한 동의로 보지 않는 등 기존과는 다른 개인정보 처리 절차 및 방법을 규정하고 있고, GDPR 시행 이전에 이루어진 개인정보 동의도 GDPR의 규정과 맞지 않는다면 다시 동의를 받도록 규정하고 있는 등 개인정보의 처리에 관하여 기존보다 한층 강화된 엄격한 규정을 두고 있어 준수하기가 매우 까다롭습니다.

EU 회원국 내 거주자를 상대로 재화나 서비스를 제공하는 기업이라면, 자신이 GDPR의 적용 대상인지, 적용 대상이라면 현재의 개인정보 처리 체계가 GDPR을 준수하는지를 신속히 점검하고 조치를 취하시는 게 좋겠습니다.

<끝>