# 2018년 5월 유럽 일반 개인정보보호 규정(GDPR) 시행 예고

EU 전역의 통일적인 개인정보보호를 위해 채택된 유럽 일반 개인정보보호 규정(GDPR- General Data Protection Regulation)은 다음 달인 2018. 5. 25. 전면적으로 시행될 예정입니다. GDPR은 EU 비회원국의 기업에게도 적용될 수 있으며 강력한 과징금 규정을 두고 있으므로 국내 기업들의 주의와 사전적인 점검이 필요합니다. 아래에서는 GDPR의 주요 내용을 알려 드립니다.

## 확장된 영토적 적용 범위(제3조)

- GDPR은 EU 내에서의 개인정보 처리 활동뿐만 아니라, ① EU 외부에서 EU 내에 위치한 정보주체에게 재화나 용역을 제공하는 경우, ② EU 내에 위치한 정보주체가 수행하는 활동을 모니터링하는 경우에도 적용됩니다.
- 이 경우에 개인정보가 처리되는 정보주체가 거주하는 회원국들 중 하나에 대리인을 지정하여야 합니다.

## 개인정보 개념의 확대(제4조)

- GDPR은 개인정보의 범위를 넓게 파악하고 있으며, IP 주소, 쿠키정보 등의 "온라인 식별자"와 위치정보도 개인정보에 해당합니다.
- GDPR은 개인정보와 익명정보의 개념을 구별하여, 익명정보는 개인정보보호의 적용대상에서 제외하여 활용가능성을 높이고 있는바, 향후 익명정보의 구체적인 범위 등이 문제될 수 있습니다.

## 개인정보 처리 원칙의 규정(제5조 등)

- 개인정보를 처리하는 경우, 컨트롤러(Controller, 우리 법상 개인정보 처리업무 위탁자와 유사)는 ① 처리의 적법성, 공정성, 투명성 원칙, ② 수집 목적 제한의 원칙, ③ 개인정보 최소화의 원칙, ④ 정확성 원칙, ⑤ 저장 제한의 원칙, ⑥ 무결성 및 기밀성 원칙 등 6가지 원칙을 준수하여야 합니다.
- 컨트롤러는 위 원칙들을 준수하였다는 사실을 증명할 의무를 부담하며, 정보주체의 동의를 받았더라도 위 6가지 원칙을 준수하여야 합니다.

## 컨트롤러의 책임 강화(제25조 등)

- GDPR은 컨트롤러의 책임을 강화하였습니다. ① 개인정보 처리 관련 세부 기록의 보관(제30조), ② 고위험 개인정보 처리에 대한 개인정보영향평가 수행(제35조), ③ 개인정보 유출 통지 및 종합적 기록 유지(제 33조, 제34조) 등의 책임을 규정하고 있습니다.
- GDPR은 Data Protection by Design and Default를 규정함으로써(제25조) 어플리케이션 등 프로그램의 개발, 설계 시점부터 개인정보처리 관련 원칙을 준수하도록 정하고 있습니다.

## 프로세서 역할 규정(제30조 등)

- GDPR은 프로세서(Processor, 우리 법상 개인정보 처리업무 수탁자와 유사)에 대해서도 ① 적절한 문서화 의무(제30조), ② 적절한 보안 기준 적용 및 정기 개인정보영향평가 수행(제32조), ③ 개인정보 국외전송 기준 준수(제5장), ④ 국가 감독기구 협조의무(제31조) 등의 의무를 부과하고 있습니다.
- 프로세서는 직접 과징금 부과대상이 될 수 있으므로, 수탁자로서 개인정보를 처리하는 경우에도 GDPR의 준수가 요구됩니다.

## 개인정보 유출 시 통지 제도(제33조)

- 컨트롤러는 개인정보 유출 발생 시, 그 사실을 알게 된 때로부터 72시간 내에 감독 당국에 신고하여야 하고, 프로세서는 개인정보 유출 사실을 알게 된 때에 컨트롤러에게 그 사실을 부당한 지체 없이 알리도록 하여야 합니다.

## 정보주체의 권리 확대(제15조 등)

- 정보주체는 ① 열람권(제15조), ② 정정권(제16조), ③ 삭제권(제17조- 잊힐 권리), ④ 처리제한권(제18조), ⑤ 개인정보 이동권(제20조), ⑥ 반대권(제21조) 등의 권리를 갖습니다.
- 기업은 GDPR에서 새롭게 도입된 제17조의 잊힐 권리, 제18조의 처리제한권, 제20조의 개인정보 이동권 등이 보장되도록 조치할 필요가 있습니다.

## 개인정보 국외 이전(제5장- 제44조~ 제50조)

- EU 내 정보주체의 개인정보를 제3국 또는 국제기구로 이전하려면, ① 제3국이 적정성 평가(Adequacy Decision)를 획득한 경우이거나, ② 개인정보를 이전하려는 기업이 적절한 보호조치(Appropriate safeguards)를 갖춘 경우 등이어야 합니다.
- 우리나라는 아직 적정성 평가를 획득하지 못하였으므로, EU 내 정보주체의 개인정보를 국내로 이전하려면, 구속력 있는 기업 규칙(Binding Corporate Rules) 또는 표준 개인정보보호 조항(Standard Contractual Clauses) 등의 적절한 보호조치 요건을 갖추거나, ③ 정보주체의 명시적 동의를 받거나 중요한 공익상의 이유가 인정되는 등의 사유가 구비되어야 할 것입니다.

## 강력한 과징금 부과 기준(제83조)

- 심각한 GDPR 규정 위반 시, 직전 회계연도의 전 세계 매출액의 4% 또는 2천만 유로 중 더 큰 금액이 과징금으로 부과될 수 있습니다.
- 일반적 GDPR 규정 위반 시, 직전 회계연도의 전 세계 매출액의 2% 또는 1천만 유로 중 더 큰 금액이 과징금으로 부과될 수 있습니다.

법무법인 세종은 행정안전부 출신 고문을 영입하는 등 개인정보 분야에 대한 독보적인 전문성과 인적 네트워크를 보유하고 있으며, EU에서 사업을 영위하는 국내 기업들을 위하여 GDPR 관련 자문을 다수 제공한 바 있고, 개인정보 규제 동향 파악 및 대관업무, 입법컨설팅, 규제영향력 분석과 기업의 전략 수립, 개인정보 보호 컴플라이언스 체계 수립 등에 대한 법률자문을 제공하고 있습니다. GDPR 및 개인정보 보호와 관련하여 보다 전문적인 내용이나 궁금하신 사항이 있으면 언제든지 연락 주시기 바랍니다.

## Contacts


| | | |
|---|---|---|
| 강신욱 파트너변호사 | TEL. 02 316 4059 | E-Mail. sokang@shinkim.com |
| 장준영 파트너변호사 | TEL. 02 316 4410 | E-Mail. jyojang@shinkim.com |
| 황정현 변호사 | TEL. 02 316 1775 | E-Mail. jhhwang@shinkim.com |