

GDPR 적용 1년의 평가

2019년 5월 21일

고려대학교 법학전문대학원
박노형 교수



GDPR 적용 1년의 평가

- GDPR은 2018년 5월 25일 적용되기 시작한 이후 세계적으로 상당한 주목을 받았음.
 - 2018년 세계 언론에서 GDPR은 Facebook 창업자인 Mark Zuckerberg 보다 더 주목을 받았다고 함. (Factiva)
 - 특히 2018년 5월 25일 GDPR이 적용되기 시작한 당일 Google에서 GDPR은 미국 슈퍼스타인 Beyonce와 Kim Kardashian 보다 더 많이 검색되었다고 함. (Google trends)
- 아래에서 수치로 검토되듯이, GDPR의 1년 적용은 대체로 양호한 평가를 내릴 수 있음.
 - GDPR은 1995년 지침과 달리 그 자체로서 EU전역에서 직접 적용되지만 허용된 예외 등의 경우 회원국들은 국내 입법을 하도록 요구하여 회원국들은 개인정보보호에 관한 자신의 국내법을 채택해야 함.
 - 예컨대, 회원국은 GDPR의 위반에 대하여 과징금이 부과되지 않는 경우에 다른 벌칙 (penalty)을 규정할 수 있음. (GDPR 제84조)
 - 불가리아, 그리스, 슬로베니아, 포르투갈과 체코는 GDPR에서 요구되는 개인정보보호에 관한 국내법을 아직 채택하지 않고 있음.

GDPR 적용 1년의 평가

- 유럽개인정보보호이사회 (EDPB)에 따르면, 2018년 5월 25일부터 첫 9개월 동안, 31개 유럽경제지역 국가들 (EEA: EU 28개 회원국들과 아이슬란드, 노르웨이와 리히텐슈타인)의 감독당국에 GDPR 관련 206,326건이 보고됨.
 - 민원 제기 건수는 94,622건이고, 침해 신고 건수는 64,684건임.
 - 이들 사건 중 1%가 회원국 국내 법원에 제소됨.
- 2018년 7월 6일 EEA공동위원회는 GDPR을 통합하는 Joint Committee Decision (JCD)을 채택하였는데, 동 결정은 2018년 7월 20일 발효하여 유럽자유무역지역 (EFTA) 국가인 경제아이슬란드, 리히텐슈타인과 노르웨이에 GDPR이 적용되기 시작함.
 - EEA국가가 아닌 스위스는 EU와의 깊은 경제적 관계를 유지하기 위하여 특히 EU로부터 '적정성 결정'을 유지하기 위하여 자신의 개인정보보호법 (Swiss Federal Act on Data Protection)을 GDPR에 일치시키도록 동 법을 개정함.

감독당국에의 민원 제기 건수

- 2019년 1월 28일 개인정보보호의 날 (data protection day 2019)을 맞이 하여 유럽위원회에 따르면, 2018년 5월 25일 GDPR의 적용 이후 2019년 1월 말 누적된 민원 제기 건수는 95,180건임.
 - 회원국 감독당국에 제기되는 민원 건수가 지속적으로 증가하는 점에서 개인들의 자신의 개인정보 보호 및 침해에 대한 의식이 높아지고 있음을 알 수 있음.
- 정보주체 즉 개인은 GDPR에 위반하여 자신의 개인정보가 처리된다고 판단하는 경우 자신의 거주지, 근무지 또는 침해 발생지의 회원국 감독당국에 민원을 제기할 수 있고, 해당 감독당국은 사법적 구제 가능성을 포함하여 해당 민원 처리 경과 및 결과를 민원인에게 고지해야 함. (GDPR 제77조 제1항과 제2항)

감독당국에의 민원 제기 건수

- 다른 회원국들에 비교하여 영국 감독당국에 월등히 많은 민원이 제기되고, 독일 및 이탈리아, 폴란드, 루마니아의 순서가 됨.
 - 그러나, 영국 (약6천7백만명)의 인구 10만명 당 민원의 건수는 51건이어서, 57건의 민원이 제기된 아일랜드 (약4백8십만명) 보다 인구당 민원 건수는 작음.
 - 아일랜드에 다수의 IT기업들 본사가 소재함: 법인세율이 12.5%로서 EU에서 최저이고 미국의 21%보다 낮아서 Google, Apple, Facebook, PayPal, Microsoft, Yahoo, eBay, AOL, Twitter, Intel 등 다수 다국적기업들이 아일랜드에 본사를 둠.
 - 폴란드 (약3천8백만명)도 인구 10만명 당 민원의 건수는 15건이어서, 29건의 민원이 제기된 헝가리 (약965만명) 보다 인구당 민원 건수는 작음.

감독당국에의 민원 제기 건수

- 회원국 감독당국에 개인이 자신의 개인정보 침해 가능성의 민원을 제기한 대표적 분야는 텔레마케팅, 홍보 이메일, CCTV/비디오 감시를 포함함.
 - 이는 ICT의 지속적인 발전으로 개인정보의 침해 가능성이 그만큼 커지고 있음을 의미함.

개인정보 침해 신고 건수

- 2019년 1월 28일 개인정보보호의 날 (data protection day 2019)을 맞이 하여 유럽위원회에 따르면, 2018년 5월 25일 GDPR의 적용 이후 2019년 1월 말 누적된 개인정보 침해 신고 건수는 41,502건임.
 - 개인정보처리자에 상응하는 컨트롤러, 예컨대 기업 등이 회원국 감독 당국에 신고하는 개인정보 침해 건수가 지속적으로 증가하는 점에서 기업 등의 개인정보보호에 대한 관심과 GDPR의 준수를 위한 노력이 증대되고 있음을 알 수 있고, 또한 개인정보 침해 건수가 지속적으로 증가하고 있음도 알 수 있음.
- 컨트롤러는 개인정보의 유출 등 침해의 사실을 안 이후 72시간 내에 소관 감독당국에게 신고해야 함. (GDPR 제33조 제1항)

개인정보 침해 신고 건수

- 영국 감독당국은 월등히 많은 개인정보 침해 신고를 받았는데, 하루 평균 42건의 침해 신고를 받음.
 - 전체 신고 건수는 영국 다음으로 아일랜드, 독일과 스웨덴, 폴란드, 헝가리 순서가 됨.
 - 영국 보다 더 많은 침해 신고 건수가 기록된 네덜란드가 반영되지 않음.
 - 아일랜드 (약4백8십만명)는 인구 10만명 당 70건의 침해 신고가 이루어짐.
 - 스웨덴은 인구 10만명 당 33건의 침해 신고가 이루어짐.

EU회원국 국경간 개인정보 처리 사건

- 2019년 1월 28일 개인정보보호의 날 (data protection day 2019)을 맞이 하여 유럽위원회에 따르면, 2018년 5월 25일 GDPR의 적용 이후 2019년 1월 말 누적된 국경간 개인정보 처리에 관련된 사건 건수는 255건이고, 최종적으로 6건의 'one-stop-shop' 사건이 확인됨.
- EU단일시장의 완성으로 SNS 서비스를 제공하는 기업 등 다수 기업들이 둘 이상의 EU회원국에서 기업 활동을 함에 따라 GDPR은 소위 협력메카니즘 또는 'one-stop-shop'원칙을 도입하여, 해당 컨트롤러, 즉 기업의 주된사업장이 있는 회원국의 감독당국 (supervisory authority)이 관련 사건을 처리하게 함. (GDPR 제56조, 제60조)
 - 해당 기업 등은 자신의 사업이 이루어지는 다수의 회원국들 감독당국들을 모두 상대하지 않아도 됨.

과징금 부과

- 유럽개인정보보호이사회 (EDPB)에 따르면, 2018년 5월 25일부터 첫 9개월 동안, 11개 유럽경제지역 국가들이 55,955,871유로의 과징금을 부과함.
 - 프랑스의 Google에 대한 과징금이 5천만유로로서 전체 과징금 금액의 절대치를 차지함.
 - 90여건의 과징금 부과 건수와 6만6천유로 평균 금액은 회원국 감독당국이 과징금 부과에 적극적이지 않은 것으로 보임.
- GDPR은 동 규정의 위반에 대한 2종류 과징금 부과:
 - 컨트롤러와 프로세서가 GDPR의 의무를 준수하지 않는 경우 1천만 유로 이하 또는 사업체의 경우 이것과 직전 회계연도의 전세계 연간매출액의 2% 이하 중 높은 금액의 과징금 부과 (GDPR 제83조 제4항)
 - 컨트롤러와 프로세서가 GDPR의 동의 조건 등 처리의 기본원칙이나 정보주체의 권리에 관한 규정을 위반하는 경우 2천만 유로 이하 또는 사업체의 경우 이것과 직전 회계연도의 전세계 연간매출액의 4% 이하 중 높은 금액의 과징금 부과 (GDPR 제83조 제5항).

과징금 부과

- 2019년 1월 28일 개인정보보호의 날 (data protection day 2019)을 맞이 하여 유럽위원회에 따르면, 2018년 5월 25일 GDPR의 적용 이후 2019년 1월 말까지 과징금 부과에 대표적 사례는 다음과 같음:
 - 2018년 9월 독일이 33만 이용자의 이메일주소를 유출한 SNS서비스 기업 Knuddels.de에게 2만유로 과징금 부과 (첫 과징금 사례);
 - 독일 LfDI는 해당 기업의 사후 협조와 투명성을 이유로 처벌 수준을 감경함.
 - 오스트리아는 불법적 비디오감시를 수행한 스포츠카페에 5,280유로 과징금 부과;
 - 프랑스는 Google에게 광고에 대한 이용자의 동의를 얻지 않은 이유로 5천만유로 과징금 부과.
- GDPR의 위반에 대하여 부과되는 과징금의 규정은 최대치에 불과하고, 해당 개인정보 처리의 성격, 위반의 성격과 중대성, 피해를 입은 정보주체의 수와 피해 정도 등 10가지 조건을 고려하여 개별 사건별로 과징금의 액수가 산정됨. (GDPR 제 83조 제2항)
 - 과징금 부과 외에 감독당국은 컨트롤러와 프로세서에게 GDPR 위반 가능성에 대한 경고, 발령 위반 컨트롤러 등에게 거쳐 발령, 준수 요청 또는 명령 등 다양한 시정조치를 부과할 수 있음. (GDPR 제58조 제2항)
 - 영국, 네덜란드, 노르웨이 보호당국은 과징금 부과에 공동체제를 마련할 것이라 함.

결어

- 2018년 5월 25일 GDPR의 적용 개시 이후 1년이 됨에 따라 GDPR의 다양한 평가가 내려지고 있는데, 대체로 EU 내에서 동법의 준수에 대한 긍정적 평가가 내려지고 있고, 세계적으로도 개인정보보호법의 개정에서 GDPR이 반영되고 있음.
- GDPR이 규정한 개인의 민원 제기 건수와 컨트롤러의 침해 신고 건수의 지속적 증가는 개인은 물론 기업 등의 개인정보보호에 대한 깊은 관심과 GDPR의 준수 노력을 보여줌.
- GDPR의 막대한 수준의 과징금 부과 규정에도 불구하고 회원국 보호당국은 GDPR을 위반한 컨트롤러 등의 사후 조치와 사안의 중요성 등을 고려하여 규정의 최대치를 부과하지 않고 있음.

결어

- GDPR은 개인정보보호에 관한 세계적 기준이 되고 있음.
 - GDPR은 EU의 28개 회원국들은 물론 아이슬란드, 리히텐슈타인 및 노르웨이 의 EFTA 회원국들에게 적용되고 있음.
 - 유럽위원회는 2019년 1월 23일 일본이 적절한 개인정보보호 수준을 보장한 과 다른 '적정성 결정' 을 채택하여 일본에의 개인정보 이동을 허용하는데, 이를 통하여 제3국의 개인정보보호법이 GDPR에 일치되고 있음.
 - 한국과 EU는 아직 적정성 결정에 합의하지 못함.
 - 유럽평의회 (Council of Europe)는 2018년 5월 18일 개인정보보호에 관한 첫 조약인 1981년 개인정보보호협약 (Convention 108)을 GDPR에 일치시키도록 '개정 의정서' (Amending Protocol)를 채택함.
 - EU는 동 'Convention 108+'에 가입할 수 있고, 동 협약에의 가입은 EU의 적정성 결정에 고려됨.
 - 미국도 주마다 다른 개인정보보호에 관한 법들을 통일하고 개인정보보호수준을 높이기 위한 연방법의 채택을 논의하고 있음.
 - 한국도 개인정보보호 관련 법률들의 개정에서 GDPR을 반영하고 있음.