해외 개인정보보호 동향 보고서

월간 보고서

2019년 3월

KISA 한국인터넷진흥원

EU GDPR 위반에 대한 벌금부과 및 유관 사례 검토

< 목 차 >

1. 개요 및 배경

▶ 2018년 5월 25일 EU의 GDPR 시행 이후 EU 회원국에서 EU GDPR(이하 GDPR) 위반 사항에 대한 벌금 부과 및 여타 유관 사례들이 축적

- EU 집행위원회(European Commission)는 GDPR 시행 이후 잠재적인 개인정보 침해 사안에 대해 9만 5,000건 이상의 불만 신고를 접수했다고 발표
- GDPR 시행 이후 영국에서만 총 20만 6,326건의 위반 사례가 보고된 가운데, 그 중 9만 4,000건에 대해 불만이 제기되었으며, 6만 4,000건이 데이터 유출 신고였던 것으로 확인
- 독일의 개인정보보호 감독기구는 GDPR 시행 이후 2019년 1월 중순까지 GDPR 위반 사안에 대해 총 41건의 벌금을 부과했으며, 최대 벌금 규모는 8만 유로였던 것으로 확인
- 프랑스의 CNIL이 Google의 GDPR 위반에 대한 대규모 벌금 부과 선례를 만든 가운데, 네덜란드, 아일랜드, 포르투갈, 덴마크, 폴란드 등 여타 회원국에서도 GDPR 위반 사례에 대한 벌금을 부과

▶ 2019년 3월 IAPP 컨퍼런스(IAPP Data Protection Intensive Conference)에서 GDPR 시행 1년에 대해 평가한 결과, GDPR 시행 후 총 5,500만 유로의 벌금이 부과되었고 그 중 5,000만 유로가 Google에 부과된 것으로 집계

- 유럽의 공공 및 민간 기업들이 2018년 5월 GDPR 시행 이후 실시한 개인정보침해 통지(notifications) 건수가 총 5만 9,000건을 기록

– 네덜란드의 개인정보 침해 통지가 총 1만 5,400건으로 가장 많았으며, 리히텐슈타인은 총 15 건에 불과해 가장 적었던 것으로 기록

▶ 이 보고서에서는 GDPR 위반에 따른 벌금부과 사례와 더불어 향후 벌금 등 제재가 이뤄질 수 있는 조사 진행 사례와 불만접수 사례를 함께 검토하기로 함

2. 주요 사례

(1) 벌금부과 사례

▶ 포르투갈의 개인정보보호 감독기구 CNPD(Comissão Nacional de Protecção de Dados)는 의료기관인 Centro Hospitalar Barreiro Montijo의 GDPR 위반 혐의로 40만 유로의 벌금을 부과[1] (`18.11)

- Centro Hospitalar Barreiro Montijo의 의사 수는 약 300명에 불과하지만, 약 1,000 명에 이르는 이들이 의사와 동일한 수준의 환자 데이터 액세스 권한을 가진 것으로 확인
- CNPD는 Centro Hospitalar Barreiro Montijo가 다음과 같은 사항을 위반하였으며 이에 따라 각각의 위반 사항에 대한 벌금을 다음과 같이 부과한다고 설명

– 다수의 사용자에게 무차별한 데이터 접근을 허용함으로써 데이터 최소화 원칙 등을 위반한 협의에 대해 15만 유로를 부과

– 개인정보에 대한 불법적인 접근을 방지하기 위한 기술적·조직적 조치를 적용하지 않은 것에 대해 15만 유로를 부과

– 해당 병원이 개인정보 처리 시스템 및 서비스의 기밀성·무결성·가용성·탄력성을 유지하지 못했던 점에 대해 10만 유로를 부과

- 한편, Centro Hospitalar Barreiro Montijo에 대한 벌금 부과는 별도의 불만 제기 등에 따른 것이 아니며 언론보도 등을 통해 파악한 내용을 바탕으로 이루어졌다는 점에서 주목

1 https://www.law.com/corpcounsel/2018/11/09/gdpr-fine-against-portuguese-hospital-puts-health-care-providers-on-alert/?slreturn=20190311130050

▶ 프랑스의 CNIL은 Google이 △사용자들에게 충분한 정보를 투명하게 공개하지 않고 △개인 맞춤형 광고에 대한 유효한 동의도 확보하지 못하는 등 EU GDPR을 위반했다며 5,000만 유로의 벌금을 부과[2] ('19.1.)

- CNIL은 Google이 데이터 처리 목적과 데이터 저장 기간에 대한 정보를 한 곳에서 제공하지 않고, 때로는 사용자가 해당 정보를 얻기 위해 5~6회 클릭하도록 한 경우도 있음을 확인
- 이와 함께 Google이 지나치게 일반적이고 모호한 설명만을 하고 있어, 명확하고 포괄적인 방식으로 정보를 제공하지도 못했다고 지적
- 특히 Google이 불충분한 정보만을 제공함으로써, 개인 맞춤형 광고에 요구되는 유효한 사용자 동의를 얻지 못했다고 판단
- 이는 GDPR 시행 후 유력 기업에 대한 첫 벌금부과 사례로서, CNIL은 Google에 대해 2018년 9월 조사 이후 상황이 전혀 달라지지 않았다는 점도 지적

▶ 폴란드의 개인정보보호 감독기구인 UODO는 정보 제공 의무를 이행하지 않은 디지털 마케팅 회사 Bisnode에게 22만 유로의 벌금을 부과 ('19.3)

- UODO에 따르면, Bisnode는 공적인 출처(public sources)를 통해 공개적으로 입수 가능한 개인 데이터를 추출하고 있다는 사실을 모든 정보주체에게 고지하지는 않은 것으로 파악
- 이는 정보주체로부터 직접 개인 데이터를 획득하지 않고 다른 경로로 확보하는 경우 해당 사실을 정보주체에게 반드시 알리도록 의무화한 제14조에 위배
- UODO는 Bisnode가 해당 사실을 고지 받은 일부 정보주체 중 13%가 이러한 데이터 처리 방식에 대해 반대했다는 사실을 언급하며, 이를 통해 성실한 고지의 의무를 제대로 이행하는 것이 얼마나 중요한 일인지 확인할 수 있다고 강조
- UNDO는 Bisnode에 대해 벌금을 부과한 것 외에도 Bisnode의 고객들이 EU GDPR 제14조의 '정보를 제공받을 권리'를 누릴 수 있도록 3개월 동안 600만 명에게 개인정보 처리 관련 사항을 알리도록 요구
- 이에 대해 Bisnode는 웹 사이트에 고지 내용을 게시했다는 점을 강조하며 수백만 통의 편지를 일일이 우편으로 고지하는 것은 시간과 비용이 많이 든다는 점을 지적했으나, UODO는 우편 고지 이외의 방법에 대한 유효성을 인정하지 않음
- Bisnode는 고객들에게 수백만 통의 편지를 발송하는 것에 대해 거부감을 피력하며,

2 https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/

폴란드의 법원에서 UNDO의 결정에 대한 사법적 판단을 요청할 계획

- 일각에서는 UODO의 이 같은 결정에 대해 EU GDPR 제14조를 문자 그대로 해석한 다소 과격한 조치였다는 평가도 제기[3]

▶ 덴마크의 개인정보보호 감독기구인 Datatilsynet은 GDPR 위반 혐의를 받는 택시 회사 Taxa 4x35에게 16만 유로의 벌금을 부과 ('19.3)

- Datatilsynet은 이 회사가 2년간의 보관 기간이 경과한 고객들의 승차 관련 정보들을 그대로 남겨두었다며, 이는 데이터 최소화의 원칙에 위배된다고 설명
- 예컨대 Taxa 4x35는 승객의 성명 정보를 삭제하면서도 전화번호는 계속 보유한 것으로 확인되었으며 Datatilsynet는 이를 근거로 벌금 부과를 결정
- 데이터를 익명화하고 고객 이름을 삭제하는 등의 노력에도 불구하고 Datatilsynet은 해당 절차가 개인정보보호를 위해서는 불충분하다고 판단했으며, 전화번호를 통해 여전히 정보주체의 식별이 가능하다는 점을 지적
- 또한 Datatilsynet은 Taxa 4×35의 기술 시스템이 관련 전화번호 없이는 승차 이력 데이터를 보존 할 수 없다는 설명도 받아들이지 않음[4]
- 이번 조치는 덴마크에서 비즈니스를 수행하는 업체들이 GDPR의 요구사항을 충족시키기 위해서는 사람들의 이름과 주소를 삭제하는 것만으로 충분하지 않으며, 벌금을 피하기 위해서는 모든 정보를 삭제해야 함을 시사

▶ 독일 바덴뷔르템베르크(Baden-Württemberg)주의 개인정보보호 감독기구(DPA)는 약 33만 명의 개인 데이터를 유출한 채팅 사이트에 대해 2만 유로의 벌금을 부과 ('19.2)

- 2018년 9월 발생한 데이터 유출로 인해 해당 개인 데이터를 해커가 공개적으로 이용할 수 있게 되었으며, 데이터 유출 통지 과정에서 사용자의 비밀번호가 암호화되지 않은 형식으로 저장되어 있었다는 사실이 공개됨
- 이에 따라 GDPR 제32조에 명시된 '적절한 보안조치'를 이행해야 할 의무를 위반한 것으로 판단하여 벌금을 부과
- DPA는 벌금부과 여부 및 벌금 규모를 결정할 때, 해당 플랫폼 제공자가 △기한 내에 DPA 및 정보주체에 위반 사실을 통보 했는가 △DPA에 대한 협조적인 태도를 유지하는가 △보안수준 강화를 위한 DPA의 권고사항을 수용하기 위해 노력하는가를 검토

3 https://techcrunch.com/2019/03/30/covert-data-scraping-on-watch-as-eu-dpa-lays-down-radical-gdpr-red-line/
4 https://www.adlawaccess.com/2019/04/articles/gdpr-recap-technical-violations-result-in-steep-fines-in-latest-enforcement-actions/

(2) 조사 진행 사례

▶ 아일랜드의 개인정보보호 감독기구인 DPC(Data Protection Commissioner)는 Facebook의 GDPR 준수 문제에 대한 조사를 개시[5] ('18.12)

- 아일랜드 DPC는 2018년 5월 25일 GDPR 시행 이후 Facebook의 개인정보보호 위반 통지를 다수 접수했으며 Cambridge Analytica 스캔들로 인해 개인정보보호와 보안 위반 문제가 반복되고 있는 것으로 판단
- 이런 가운데, Facebook의 엔지니어 담당 이사인 Tomer Bar는 외부 애플리케이션에 데이터가 노출되는 버그로 인해 서드파티 개발자가 Facebook 가입자의 개인 사진에 액세스 할 수 있는 문제가 발생했다고 시인
- 해당 버그로 인해 2018년 9월 13일부터 9월 25일까지 12일 동안 잠재적으로 최대 680만 명의 사용자가 영향을 받았을 것으로 추정
- 이에 따라 Facebook은 대형 기술기업으로는 처음으로 아일랜드 DPC로부터 GDPR 위반 가능성에 대한 조사를 받게 되었으며, 앞으로 DPC는 개인정보 침해로 인해 실제로 영향을 받은 사용자들에 대한 조사를 진행할 전망[6]
- 한편, 아일랜드 DPC는 2018년 12월 31일 기준으로 다국적 기술 기업에 대해 15건의 조사를 진행하고 있으며, 그 중 10건은 Facebook 및 자회사인 Instagram과 WhatsApp에 관한 것이라고 발표[7]

▶ 아일랜드 DPC는 소셜 미디어 업체 Twitter로부터 개인정보침해 통지를 받은 후 관련 조사를 시작[8] ('19.1)

- DPC는 2019년 1월 8일 Twitter로부터 데이터 유출 관련 통지를 받았으며 그에 따라 관련 조사를 진행하되 이번 조사에서는 Twitter가 GDPR 제33조를 준수했는지 여부에 대한 사항들을 검토한다고 설명
- GDPR 제33조는 개인정보침해 발생 시 이를 인지한 후 72시간 이내에 개인정보보호 감독기구에게 통지할 것을 명시
- 한편, DPC는 Twitter와 관련해 제기된 또 다른 개인정보침해 사안들에 대해 2018년 11월부터 조사를 진행하고 있는 상황

5 https://www.ft.com/content/d796b5a8-ffc1-11e8-ac00-57a2a826423e
https://www.independent.ie/business/technology/news/facebook-faces-billioneuro-fine-as-irish-data-protection-commissioner-opens-fresh-investigation-into-photo-leak-37627547.html
6 https://www.bloomberg.com/news/articles/2019-02-01/facebook-faces-seven-data-probes-as-irish-watchdog-gets-tough
7 https://www.documentcloud.org/documents/5753493-DPC-Annual-Report-25-May-31-December-2018.html
8 https://www.reuters.com/article/us-twitter-cyber-ireland/irish-data-watchdog-investigates-twitter-over-privacy-rules-breach-idUSKCN1PJ28G

▶ 영국의 개인정보보호 감독기구 ICO는 Google 및 데이터 수집에 대한 수많은 불만이 접수됨에 따라 Google의 '강제동의(forced consent)' 방식이 GDPR에 저촉되는지 여부를 조사[9] ('19.2)

- 개인정보보호 옹호 단체들은 팝업 상자를 통해 강제동의를 푸시(push)하는 이러한 방식에 대해 GDPR 발효 직후부터 불만을 제기
- 이에 따라 특히 웹 사이트와 앱 이용을 위해서는 데이터 수집에 동의하는 것 외에 다른 선택의 여지가 없도록 한 것의 위법성 여부를 검토해야 한다는 의견이 제기
- 이런 가운데, ICO는 Google과 관련한 다양한 불만 사항이 접수된 후 유럽 전역의 여러 규제기관들과 함께 추진할 수 있는 대응 조치를 모색 중

(3) 불만 접수 사례

▶ 개인정보보호 운동가인 Max Schrems와 시민단체 NOYB(None Of Your Business)는 주요 온라인 스트리밍 서비스가 GDPR을 위반하고 있다며 오스트리아 개인정보보호 감독기구인 DPA에 불만을 제기 (`19.1.)

- Schrems와 NOYB는 Amazon Prime, Apple Music, Netflix, SoundCloud, Spotify, YouTube, Austria Flimmit, DAZN 등 8개 스트리밍 서비스 업체가 GDPR 제15조 정보주체의 열람권 행사에 필요한 모든 고객 데이터를 제공하지 못하고 있다고 지적
- Schrems에 따르면, 많은 스트리밍 서비스들이 열람권 요청에 응답하는 자동화 시스템을 구축했으나 이를 통해 데이터를 제대로 제공하지 못하는 상황
- 대부분의 경우 원시 데이터만 제공될 뿐 해당 데이터가 누구와 공유되었는가에 대한 정보는 공개되지 않는 등 정보주체의 권리 행사를 구조적으로 저해
- 한편, 일반적으로 스트리밍 서비스는 추천 서비스 제공, 사용자의 전반적인 취향 파악, 광고 판매 등을 위해 사용자의 데이터를 이용한다는 점에서 GDPR 위반 가능성에 대한 각별한 주의가 필요

▶ 개인정보보호 옹호 단체들은 광고 비즈니스 업계 단체인 IAB(Internet Advertising Bureau)와 Google이 GDPR을 위반했다며 영국 ICO와 아일랜드 DPC(Data Protection Commission)에 신고[10] ('19.2)

- Google과 IAB가 사용하는 실시간 광고 입찰((RTB) 시스템은 GPS 위치와 사용자의 웹 브라우징 이력 등 주요 개인 데이터를 하루에 수십억 회씩 공유

9 https://www.theinquirer.net/inquirer/news/3070441/ico-google-gdpr-probe
10 https://www.internetsecuritycentral.com/privacy-activists-say-online-ad-industry-knowingly-violated-gdpr/

- RTB 시스템은 웹 사이트에 광고가 게재되기도 전에 입찰에 참여하는 제3자 업체와 개인 데이터를 공유하게 된다는 점에서, 개인정보처리 목적과 관련해 '정보에 입각한 동의'가 불가능하다는 것이 이 단체들의 주장
- 이번 신고 과정에서 제출된 문서에는 IAB가 RTB 시스템의 GDPR 위반 가능성을 이미 인지하고 있었음을 시사하는 문서도 포함

(4) 기타 사례

▶ 개인정보보호 옹호단체인 Privacy International은 Facebook과 광고주들이 GDPR을 위반했을 가능성이 있다고 지적[11] ('19.1)

- Privacy International에 따르면, Facebook이 제공하는 소프트웨어 개발 키트 (SDK)를 사용한 앱에서는 데이터가 자동으로 Facebook으로 전송
- 사용자가 동의하지 않았거나 계정에서 이미 로그아웃했거나 심지어 Facebook 계정을 가지고 있지 않은 경우에도 안드로이드 앱 개발자가 Facebook과 데이터를 공유하는 기능이 작동하는 것으로 확인
- 지금까지 Facebook의 개인정보보호 위반 사례는 GDPR 시행 이전에 발생한 사안이라는 이유로 이전 법규에 따라 처리되는 한계가 있었으나, 이번 Privacy International의 조사 내용이 입증될 경우 GDPR과 연계할 수 있는 사례가 될 전망
- 한편, GDPR에서는 기업이 개인정보를 수집하는 구체적이고 정당한 이유가 있어야 한다는 점을 명확히 하고 있으나, Facebook은 구체적 목적이나 타당한 이유가 없더라도 일단 사용자에 대한 정보를 수집하는 것으로 추정

▶ 영국에서는 차량공유서비스 업체 Uber가 운전자들에게 정보열람권을 보장하지 않아 GDPR을 위반했다는 혐의로 피소 ('19.3)

- 운전자들은 Uber를 상대로 운전자 자신의 평가 등급, 개별 GPS 데이터, Uber 플랫폼에 로그인한 시간 등 정보주체로서 요구할 수 있는 데이터를 제공해달라고 요청했으나 Uber가 이를 이행하지 않았다고 주장
- GDPR에 따라 정보주체 개인은 고용주와 회사가 보유한 자신의 개인 데이터에 접근할 권리가 있으며, 회사는 이러한 요청에 대해 1개월 이내에 구두 또는 서면으로 응답하는 것이 의무
- 운전자들은 이 같은 Uber의 행태에 대해 비판하며 법원에서 시비를 가리기 위해 소송을 제기

11 http://telecoms.com/494395/privacy-international-points-gdpr-finger-at-facebook/

3. 결론 및 시사점

▶ 현재까지의 벌금부과 사례와 조사 진행 및 불만제기 사례 등은 GDPR에서 요구하는 "적절한" 안전 조치를 이행하고 데이터 유출 사고 발생 시 신속하고 정확한 고지 의무를 다하는 것이 필수 조건임을 시사[12]

- 데이터 저장 시 암호화 처리 및 개인정보에 대한 접근권한 관리를 위한 식별 및 인증 등의 안전 조치들이 이루어지지 않았을 경우, 데이터 유출 사고 등의 문제 발생 시 벌금으로 이어질 가능성이 높아짐
- 문제가 발생하더라도 개인정보보호 감독기구(DPA)와 적극적으로 협력할 경우 벌금 산정에 긍정적인 영향을 기대할 수 있으며, 개인정보보호 위반 사실이 파악되는 즉시 DPA에 통지하고 완전한 협력 태세를 확보함으로써 사태 수습에 도움을 받을 수 있음

▶ 한편, GDPR 위반 사례에 대한 벌금부과 초기 단계에서 각국 DPA들은 새로운 GDPR 요구사항을 준수하지 않는 경우를 대규모로 발굴해 벌금을 부과하기보다는 기본적인 의무사항조차 충족하지 못하는 소수의 사례를 집중적으로 공략하는 특징을 보였음[13]

- 따라서, 당분간 기업 및 조직에서 GDPR 준수를 위한 실행 전략을 세울 때는 가장 중요한 요구사항에 우선순위를 둘 수 있도록 명확한 방침을 설정하는 것이 중요하다고 판단됨

Reference

1.Ad Law Access, GDPR Recap: Technical Violations Result in Steep Fines, In Latest Enforcement Actions, 2019.4.3
2. Cnet, Google fined $57 million under new European data privacy law, 2019.1.21.
3. Financial Times,Facebook faces fresh probe after photo leak, 2018.12.15
4. IAPP, First GDPR fine in Portugal issued against hospital for three violations, 2019.1.3.
5. Polish DPA issues the first fine for a violation of the GDPR,Lexology, 2019. 4. 3.
6. Privacy International, How Apps on Android Share Data with Facebook – Report, 2018.12월
7. Takeaways from the First GDPR Fines, Lexology, 2018.12.18

12 출처: https://www.lexology.com/library/detail.aspx?g=a91ba97a-eae9-408c-a53f-c47d1c6d62ea
13 출처: https://www.lexology.com/library/detail.aspx?g=a91ba97a-eae9-408c-a53f-c47d1c6d62ea

2019년 3월

KISA 한국인터넷진흥원

KISA 한국인터넷진흥원

발 행 일 2019년 3월
발 행 및 편 집 한국인터넷진흥원 개인정보보호본부 개인정보정책기획팀
주 소 전라남도 나주시 진흥길 9 빛가람동 (301-2) Tel 1544-5118