해외 개인정보보호 동향 보고서

월간보고서 2019년 11월

KISA 한국인터넷진흥원

아일랜드 DPC의 클라우드 서비스 이용관련 가이드라인 주요 내용 및 분석

< 목 차 >

1. 개요 및 배경

▶ 제3자의 플랫폼에 데이터를 저장하는 클라우드 저장 서비스(이하 클라우드 서비스)와 관련하여 개인정보보호 문제가 중대한 이슈로 부각

- 클라우드 서비스란 “문서, 사진, 동영상, 기타 파일을 원격 서버에 저장해 공유 또는 원격 접속할 수 있도록 하는” 것을 의미[1]
- 소프트웨어 보안업체 McAfee에 따르면, 클라우드에 저장된 데이터 중 약 4분의 1이 민감한 개인정보로 추정되며, 평균적으로 월 2,200건 이상의 구성 오류(misconfiguration) 사고가 발생[2]
  - 예컨대, 의도하지 않은 상태에서 다른 서비스와 우연히 데이터가 공유되거나 클라우드 서비스의 구성 오류 및 보안 위협이 모두 증가한 것으로 확인

1 https://www.dataprotection.ie/en/guidance-landing/guidance-organisations-engaging-cloud-service-providers
2 https://apnews.com/941c097b39b4434e84584280afb970d3

• 이러한 클라우드 환경에서 개인정보보호를 위해 데이터 처리 과정의 기술적·관리적 보호조치를 강화하기 위해서는 각별한 노력이 필요

– GDPR 시행으로 조직은 데이터 관리 정책을 마련해야 하며, 특히 제3자가 데이터에 접속하는 경우 고객의 개인정보를 보호하기 위해 이러한 데이터의 구성, 보유, 이용 방식은 더욱 엄격하게 관리되어야 함

▶ 아일랜드의 개인정보보호 감독기구 DPC(Data Protection Commission)는 클라우드 서비스 이용 가이드라인(Guidance for Organisations Engaging Cloud Service Providers)을 발표

• DPC의 가이드라인은 비즈니스 목적으로 클라우드 서비스를 이용하는 조직이 개인정보 처리와 관련해 보안 및 개인정보보호를 강화해야 한다는 관점에서 작성된 것이 특징

• DPC의 가이드라인은 △클라우드 서비스(클라우드 컴퓨팅) 개요 △클라우드 환경에서 보안과 관련하여 고려할 사항 △투명성 △개인정보의 저장 위치 △클라우드 서비스의 계약 조건 △EDPS와 ENISA 등 EU의 다른 기구들이 제시하는 기타 가이드라인에 대한 소개 등으로 구성

• DPC의 가이드라인은 데이터 컨트롤러가 △EU GDPR에 따라 클라우드 상에서 정보처리에 대한 투명성을 확보하고 △클라우드 서비스 제공자와 개인정보보호를 위한 적절한 계약을 체결할 것을 권고

• 본 보고서에서는 DPC의 가이드라인 핵심 내용을 검토 및 분석하고 클라우드 환경의 개인정보 침해 사례 등을 함께 검토

2. 가이드라인의 주요 내용

(1) 클라우드 환경에서 개인정보처리의 특징

▶ 개인정보를 처리하는 조직(데이터 컨트롤러)이 제3자의 서버 또는 데이터센터 등에서 정보처리의 일부 또는 전체 업무를 수행하는 클라우드 서비스 이용이 확산됨에 따라 클라우드 환경에서의 개인정보보호 중요성 심화

• 제3자 클라우드 서비스 사업자는 대체로 데이터 컨트롤러를 대행하여 데이터 프로세서의 역할을 수행하며, GDPR의 요구사항에 대한 책임을 준수

※ 데이터 프로세서는 데이터 컨트롤러를 대신하거나 그 지시에 따라 개인 정보를 처리하는 개인 또는 조직을 의미

• 클라우드 사업자는 일반적으로 데이터 컨트롤러에게 정보처리 대행 서비스를 제공하지만, 클라우드 사업자 자신이 데이터 컨트롤러 혹은 공동 데이터 컨트롤러(joint controllers)의 역할을 할 수 있으며 이 경우에는 데이터 컨트롤러로서 더 엄격한 GDPR 준수 책임이 부과

(2) 클라우드 환경에서 보안과 관련하여 고려할 사항

▶ 데이터 컨트롤러가 클라우드 사업자에게 개인정보 처리를 위탁하는 경우, 다음과 같이 개인정보의 안전과 데이터 보안 확보를 위한 조치가 필요

- GDPR 제28(1)조에 따라, 개인정보보호를 위한 적절한 기술적·관리적 조치를 이행할 수 있고 정보주체의 권리 보호를 충분히 보증하는 클라우드 서비스 제공자를 선택
- GDPR 제32조에 따라, 데이터 컨트롤러와 데이터 프로세서가 개인정보 침해 위험에 대한 적정 수준의 보안을 확보하기 위해 적절한 기술적·관리적 조치를 이행
- GDPR 제40조(승인된 행동 강령)[3]와 GDPR 제42조(승인된 인증 메커니즘)[4]에 따라 작성된 행동강령과 모니터링을 통해 제32조의 의무를 보완
- 이러한 맥락에서 클라우드 서비스 이용과 관련해 데이터 컨트롤러가 주목해야 할 보안의 두 가지 주요 측면은 다음과 같음
  - 첫째, 데이터 프로세서(클라우드 사업자)가 데이터 컨트롤러의 통제와 지침에 따라서만 정보를 처리할 것이라는 점을 확신할 수 있어야 하며, 이는 데이터 컨트롤러와 클라우드 사업자 사이의 계약 내용에 반영
  - 둘째, 전송·저장·처리되는 개인정보가 우발적 또는 불법적으로 파괴·손실·변경·무단 공개·액세스로 인해 위험에 처할 수 있다는 사실을 클라우드 사업자가 충분히 고려하고 있다고 확신할 수 있어야 함

▶ 클라우드 사업자에게 개인정보 처리를 위탁하기에 앞서 데이터 컨트롤러는 클라우드 사업자의 보안 표준이 충분하고 적합하다는 점을 확신할 수 있어야 하며, 이와 관련 클라우드 사업자는 다음과 같은 주요 사안들에 대해 보장하는 것이 필요

- 첫째, 필요한 경우 개인 정보의 가명화 및 암호화함으로써 제3자의 접속으로부터 데이터 보안을 유지하고 데이터 유출 사고가 발생할 경우에도 재식별이 어렵도록 조치
- 둘째, 당해 데이터 컨트롤러가 제공한 개인정보를 클라우드 사업자의 다른 고객들이 제공한 정보로부터 격리 또는 분리하도록 조치
- 셋째, 데이터 처리 시스템과 서비스에 대해 지속적으로 기밀성·무결성·가용성·탄력성을 보장하는 조치가 필요하며, 여기에는 직원의 기밀 누설을 방지하는 것부터 GDPR

3 GDPR은 회원국, 감독기관, 유럽정보보호이사회, 집행위원회는 다양한 처리 부문의 명확한 특징과 영세 및 중소기업의 특정 요구를 고려하여 본 규정을 적절히 적용하기 위한 취지의 행동강령을 입안하도록 장려하고 있으며, 데이터 컨트롤러나 데이터 프로세서의 각 범주를 대표하는 협회(associations) 또는 기타 기관은 행동강령을 제정하거나 해당 강령을 수정 또는 확대할 수 있음

4 GDPR 제40조에 따른 행동강령의 준수에 대한 모니터링은 행동강령의 주제와 관련하여 적정 수준의 전문지식을 보유하고, 관련 감독기관이 그 목적으로 승인한 기관이 실시할 수 있음

제32조의 보안 요건을 충족하는 것에 이르기까지 다양한 기술적·관리적 수단들이 포함

- 넷째, 물리적 또는 기술적 사고 발생 시 적시에 개인 정보의 가용성과 접근성을 복구하는 역량을 확보
- 다섯째, 정보 처리의 보안을 위해 채택한 기술적·관리적 수단의 효과성을 정기적으로 시험 및 평가하는 프로세스를 마련
- 여섯째, 개인정보 침해 사고 발생 시 실질적인 사고 대응이 가능하도록 계획을 수립하고, 데이터 컨트롤러와 데이터 프로세서 사이에 개인정보 침해 통지에 대한 구속력 있는 계약을 체결함으로써 정보주체가 불필요하게 위험에 처하지 않도록 조치
- 일곱째, 클라우드 서비스 계약 종료 시 모든 개인정보를 삭제하거나 데이터 컨트롤러에게 반환하기 위한 수단을 확보

(3) 투명성

▶ 데이터 컨트롤러가 클라우드 사업자의 GDPR 준수 사실을 확인하고, 정보주체에게 클라우드 사업자를 통한 개인정보처리 사실을 공개할 수 있도록 투명성을 확보하는 것이 필요

- GDPR 28(3)(h)조에 따라, 클라우드 사업자는 GDPR 준수를 입증하는데 필요한 일체의 정보를 개인정보처리자에게 제공하고 감사 활동에 협조
- 이 같은 의무를 수행하기 위해서는 클라우드 사업자에 대한 감사 설문(audit questionnaire) 실시로 충분할 수 있으며, 보안 약정 문제가 이 같은 감사의 핵심
- 개인정보 처리활동에 대한 기록을 유지하도록 한 GDPR30(2)조의 요구사항은 클라우드 사업자에 대해서도 적용되며, 클라우드 사업자는 GDPR이 요구하는 책임성 준수의 일환으로 지정된 기본 정보를 문서화하고 해당 내용을 데이터 컨트롤러에게 제공
- GDPR 제28(2)조 및 28(4)조에 따라, 클라우드 사업자는 데이터 컨트롤러의 승인 없이 다른 데이터 프로세서를 고용하는 경우 해당 사안에 대한 정보를 데이터 컨트롤러는 물론 데이터 컨트롤러의 고객에게도 제공하는 것이 의무
  - 이를 통해 데이터 컨트롤러는 계약 조건에 따라 이러한 약정을 검토할 수 있으며, 다른 데이터 프로세서를 통한 개인정보 처리에 반대할 수 있음
- GDPR 제 28(5)조는 데이터 프로세서가 개인정보 처리의 적합성을 입증하기 위해 GDPR 제40조와 제42조에 명시된 '승인된 행동 강령' 또는 '승인된 인증 메커니즘'을 활용할 수 있다고 명시하고 있으며, 데이터 프로세서로서 클라우드 사업자는 이러한 행동 강령 또는 인증의 성격, 범위, 맥락에 대한 정보를 데이터 컨트롤러에게 명확하게 제공하는 것이 필요
  - 이를 통해 데이터 컨트롤러는 해당 행동 강령과 인증 메커니즘이 개인정보 처리 작업에 적용되는 정도를 이해할 수 있음

(4) 개인정보의 저장 위치

▶ EU 시민들의 개인정보가 유럽연합 역외 지역에 위치한 클라우드 서버에 저장되는 경우에는 개인정보보호를 위한 특별한 조치가 필요[5]

- 유럽경제지역(European Economic Area, EEA)[6] 역내에 위치한 클라우드 서버에 저장된 개인정보는 EU 수준에서 규정된 공통 보호 표준에 따라 보호
- 클라우드 사업자가 EEA 외부에서 개인 정보를 처리하는 경우, GDPR에 의거하여 △적정성 결정에 따른 이전(제45조) △적정한 안전조치에 의한 이전(제46조) △구속력 있는 기업 규칙(제47조)에 따른 이전 등이 가능[7]
- 개인정보의 역외 이전을 위한 표준 개인정보보호 조항이나 BCR이 적용되는 경우, 이러한 메커니즘이 제공하는 보호 장치는 클라우드 사업자가 계약을 맺은 모든 하도급 데이터 프로세서에게도 적용

(5) 클라우드 서비스의 계약 조건

▶ 데이터 컨트롤러가 클라우드 사업자를 데이터 프로세서로 활용하는 경우, 클라우드 사업자를 통해 처리되는 개인정보에 대한 통제 권한은 데이터 컨트롤러에게 있으며 클라우드 사업자와의 계약에 다음과 같은 요점들을 포함시킬 것을 권고

- 첫째, 클라우드 사업자와 당해 클라우드 사업자의 하도급을 맡은 데이터 프로세서는 데이터 컨트롤러의 지시에 의해서만 정보를 처리해야 함
- 둘째, 클라우드 사업자는 보안 조치 및 GDPR 제32조(개인정보처리의 보안)의 요구사항 충족 방안에 대한 상세한 보증을 제공해야 함
- 셋째, 클라우드 사업자는 현재 이용 중인 하도급 처리자의 목록 및 하도급 처리자의 목록이 업데이트되는 경우 데이터 컨트롤러가 이에 대응할 수 있는 방식에 대한 세부사항을 제공해야 함
- 넷째, 클라우드 사업자의 GDPR 제28조 준수 사실 증명에 필요한 정보 및 데이터 프로세서에 대한 데이터 컨트롤러의 감사 및 검사를 수용하고 협조하기 위한 방안을 제공해야 함

5 글로벌 대기업들이 거대한 데이터 센터로 구성된 "클라우드" 네트워크를 운영하는 시대에는 개인의 데이터가 어디에나 저장될 수 있다는 현실을 반영

6 EU 회원국들에 아이슬란드, 리히텐슈타인 및 노르웨이가 추가됨

7 GDPR에 따르면, EU 역내로 개인정보 이전이 가능한 경우는 ① 적정성 결정(Adequacy Decision) ② 표준 개인정보보호 조항(Standard Data Protection Clauses) ③ 구속력 있는 기업 규칙(BCRs, Binding Corporate Rules) ④ 승인된 행동규약(Codes of Conduct) 및 인증제도(Certicifation mecahnism) ⑤ 특정 상황에 대한 예외(Derogations for specific situations) 등이 있음 (출처: 우리 기업을 위한 GDPR 안내서)

- 다섯째, EEA 외부에서 처리되는 개인정보의 보안을 보장하기 위한 조치가 제시되어야 함
- 여섯째, GDPR 위반 및 개인정보 발생 시 데이터 컨트롤러와 데이터 프로세서의 책임 범위 배분 및 데이터 컨트롤러에게 침해사실을 통지하는 방법이 명시되어야 함
- 일곱째, 데이터 프로세서가 정보주체의 권리 행사를 지원하기 위한 방법이 제시되어야 함
- 여덟째, △개인정보 처리의 주제, 범위, 성격, 맥락, 목적, 기간 △개인정보 수명주기에 따라 처리되는 개인정보의 유형과 범주 등이 제시되어야 함

(6) 기타 가이드라인

▶ 유럽연합의 개인정보보호 감독기구 EDPS(European Data Protection Supervisor)는 유럽 내 각종 기관과 조직들을 대상으로 클라우드 컴퓨팅 서비스를 사용하는 최선의 방법을 제시한 가이드라인(Guidelines on the use of cloud computing services by the European institutions and bodies)을 발표('18.3.16)

- 이 가이드라인은 개인정보가 클라우드 기반 서비스로 처리 될 때 기업이 직면하게 될 데이터 보호 및 개인정보 위험요소를 평가하고 관리할 수 있도록 도움을 제공하기 위한 목적으로 작성
- 유럽 일반 개인정보보호법(GDPR)과 관련된 관련 규정을 강조하고, △클라우드 컴퓨팅이 적절한 옵션인지 여부에 대한 평가 △데이터 보호 요구사항을 검토하고 고려하여 적절한 클라우드 컴퓨팅 옵션을 결정하는 방법 △관련 조직 및 기술적 인 안전장치 등에 대해 설명
- 또한 가이드라인의 부록에서는 용어설명, 추가적인 법률 분석, 클라우드 컴퓨팅의 기초개념과 모델, 데이터보호와 관련한 클라우드 컴퓨팅의 위험, 참고자료 등을 제시

▶ EU 산하 정보보호기구인 ENISA(European Union Agency for Network and Information Security)는 다음과 같은 두 가지 가이드라인을 제시

- 첫째, '클라우드 및 IoT의 안전한 융합을 위한 가이드라인(Towards secure convergence of Cloud and IoT)'을 통해, IoT 생태계에서 클라우드 상에 발생하는 보안 문제를 식별하고 해결하기 위한 접근 방안을 간략하게 제시('18.9.17)
- 둘째, '디지털 서비스 사업자를 위한 최소 보안 조치의 구현을 위한 기술 지침(Technical Guidelines for the implementation of minimum security measures for Digital Service Providers)'을 통해, 유럽 지역의 디지털 서비스 사업자들에 대한 최신 정보 및 네트워크 보안 관행을 조사하고 DSP의 보안 조치에 관한 일반적인 접근 방식을 제시('17.2.16)
- 셋째, '중소기업을 위한 클라우드 보안 안내(Cloud Security Guide for SMEs)'를 통해, 중소기업이 클라우드 서비스를 이용할 때 고려해야 할 보안 위험과 기회에 대해 설명 ('15.4.10)

3. 참고: 클라우드 환경의 개인정보 침해 및 대응 사례

(1) 개인정보 침해 사례

▶ Amazon의 클라우드 서비스인 AWS(Amazon Web Services) S3 스토리지 버킷의 설정 오류로 수많은 소비자들의 금융 거래 내역, 연락처 정보, 모기지 대출에 대한 중요한 데이터가 노출되는 사고가 발생

- 보안전문업체 Upguard의 사이버 리스크 팀은 AWS 계정만 있으면 누구든지 마케팅 및 분석 회사 Alteryx의 데이터베이스를 들여다볼 수 있도록 되어 있음을 확인
- Alteryx가 AWS의 모든 '허가된 이용자(Authenticated Users)'에게 자사 데이터베이스를 다운로드 받을 수 있도록 권한을 잘못 설정한 것이 사고의 원인
- 이에 따라 Alteryx의 제휴사인 신용평가업체 Experian과 미국 인구조사국(US Census Bureau)의 데이터셋도 알터릭스 데이터베이스를 통해 대량 노출
- 노출된 데이터에 이름은 포함되지 않았으나 연락처, 인종, 학력, 수입, 자녀, 대출 관련 세부정보 등 금융정보와 사생활 정보가 포함된 것으로 확인
- 미국의 신용정보사 Equifax의 고객정보 대량유출 사태에 이어, 미국의 1억 2,300만 가구 구성원들의 개인정보가 온라인에 방치되었다는 점에서 사회적 파장이 큰 사건으로 평가

▶ 리서치 전문 업체 Deep Root Analytics가 1억 9,800만 명에 달하는 미국 유권자들의 개인정보를 누구나 접속할 수 있는 아마존 클라우드 서버에 스프레드시트 형태로 보관해온 사실이 확인

- 해당 데이터에 대해서는 비밀번호나 기타 보안 프로토콜 없이 접속이 가능했으며, 약 1.1 테라바이트에 달하는 유출된 자료에는 미국 인구의 62%에 달하는 유권자들의 집주소, 생년월일, 전화번호 등의 개인정보와 정치적 성향 등이 포함
- Deep Root Analytics는 자사의 전적인 책임을 인정하면서 시스템이 해킹된 것은 아니며, 사태를 전달받은 이후 추가 접속을 방지하기 위한 보안 프로토콜을 설정했다고 강조
- 그러나 Deep Root Analytics가 여러 공적/상업적 기관을 통해 자료를 수집한 것으로 알려지면서 개인정보를 광범위하게 수집해 유권자의 정치적 견해를 예측하거나 변화시키고자 하는 활동이 시민들의 프라이버시를 위협한다는 우려가 제기된 사례

(2) 개인정보침해 방지를 위한 대응 사례

▶ Microsoft는 GDPR 위반 가능성에 대한 조사가 시작된 후 Azure 클라우드 서비스의 개인정보보호 기능 강화를 위한 온라인 서비스 약관(Online Services Terms, OST) 내용을 개정

- EDPS는 EU의 주요 기관들과 Microsoft의 클라우드 계약 내용 및 GDPR 준수 현황에 대한 조사 결과를 발표하며 "심각한 우려"를 표명
- Microsoft가 Office 365 ProPlus와 Office 365 사용자로부터 원격 데이터를 수집하는 것과 관련, GDPR 위반 소지가 있다는 네덜란드 법무부의 판단에 따라 2019년 4월부터 EDPS가 조사에 착수
- 이후 Microsoft가 계약 내용을 새롭게 개편하고 정보주체의 권리 침해 위험을 완화하는 조치를 취하기로 네덜란드 법무부와 합의했으며, EDPS는 2019년 10월 이를 "긍정적인 진전"이라고 평가
- Microsoft는 네덜란드 법무부와의 합의 내용을 반영하여 Azure 서비스의 모든 상용 고객을 위한 온라인 서비스 약관(OST) 계약에 새로운 개인정보보호 조항을 추가한다고 발표
- 고객에게 Microsoft 클라우드의 데이터 처리에 대한 정보를 투명하게 제공하도록 한 새로운 약관은 기업의 규제 준수를 압박한 규제 당국의 역할을 보여주는 대표적인 사례이며, Microsoft의 대응 조치로 인해 EDPS의 조사에도 영향을 미칠 것으로 전망

▶ Amazon의 클라우드 서비스인 AWS(Amazon Web Services)는 클라우드 서비스 비즈니스와 관련해 GDPR을 철저하게 준수하기 위한 노력을 지속

- 약 20개의 클라우드 인프라 제공업체들이 참여하는 CISPE(The Cloud Infrastructure Services Providers in Europe)에 합류한 것이 대표적인 사례
- 이와 관련, 서비스 레벨에서 Amazon EC2, Amazon S3, Amazon RDS, AWS Identity and Access Management, CloudTrail, Amazon EBS 등 AWS의 6가지 클라우드 제품이 CISPE 행동 규범을 준수한다는 인증을 획득
- AWS는 이를 통해 고객업체들이 AWS를 이용할 때 안전하고 보안과 규제 컴플라이언스가 완비된 환경에서 데이터를 완벽하게 제어할 수 있다는 것을 추가적으로 보장
- 한편, CISPE의 목표에는 기업의 행동규범(Code of Conduct)을 통해 업계 전반적으로 GDPR을 준수하도록 지원하는 것이 포함
  - CISPE는 클라우드 인프라 서비스 제공업체를 위한 데이터 보호 행동 강령(Data Protection Code of Conduct)을 발표하면서 이미 이 분야에서 상당한 발전을 이룬 것으로 평가

4. 시사점

▶ 클라우드 서비스 환경에서 개인정보보호의 문제는 데이터 컨트롤러가 제3자 데이터 프로세서에게 개인정보 처리를 위탁하는 과정에서 개인정보보호 및 보안을 위한 충분한 기술적·관리적 조치를 취하는 것이 핵심 과제

- 아일랜드 DPC가 지적한 바와 같이, 개인정보보호 및 보안에 대한 위험은 △데이터 컨트롤러가 개인정보에 대한 통제 권한을 클라우드 서비스 사업자에게 이양하는 경우 △클라우드 서비스의 데이터 처리 방식 및 보호 장치에 대한 정보가 투명하게 공개되지 않는 경우 △클라우드 서비스 사업자가 GDPR에 명시된 의무 사항을 충분히 수행하지 않거나 정보주체의 권리를 충분히 지원할 수 없는 경우에 발생
- 이와 관련, DPC의 가이드라인은 개인정보보호를 위한 핵심 요소 중 하나로 보안의 중요성을 지적하고, 정보처리의 투명성과 EU 역외지역으로의 개인정보 이전 조건, 클라우드 서비스 계약에 반드시 포함되어야 할 요소들을 강조함으로써 클라우드 환경에서 개인정보보호 강화 방안을 제시

Reference

1. AP, “New McAfee Report Reveals Data in the Cloud More Exposed Than Organizations Think”, 2018.10.30.
2. DPC, "Guidance for Organisations Engaging Cloud Service Providers", 2019.11월 접속
3. EDPS, “Guidelines on the use of cloud computing services by the European institutions and bodies”, 2018.3.16
4. PC Magazine, “Google Beefs Up Cloud Security and Data Privacy Tools”, 2018.3.21
5. ZDNet, “Microsoft: We're changing all your cloud contracts after privacy complaints”, 2019.11.18

KISA 한국인터넷진흥원

발 행 일 2019년 11월
발 행 및 편 집 한국인터넷진흥원 개인정보보호본부 개인정보정책기획팀
주 소 전라남도 나주시 진흥길 9 빛가람동 (301-2) Tel 1544-5118