해외 개인정보보호 동향 보고서

최신동향 보고서 2017년 5월 4주

KISA 한국인터넷진흥원

영국 ICO, GDPR 시행에 대비한 12가지 조치사항 발표

1. 배경 및 목적

▶ 영국 정보보호위원회(ICO)는 2018년 5월 25일부터 시행될 EU GDPR에 대응하기 위해 필요한 12가지 조치사항(Checklist)을 발표[1] (3.13)

- GDPR의 주요 개념과 원칙들 중 상당수는 영국의 현행 데이터보호법(Data Protection Act, DPA) 내용과 거의 동일하므로, 현행법을 제대로 준수하고 있다면 GDPR 프레임워크에서도 대부분의 기존 방식은 유효
- 그러나 GDPR에 새롭게 추가된 요소와 중요한 개선사항이 있으므로 처음에는 이에 부합하도록 몇 가지 작업을 해야 하고 기존과는 달라진 방식으로 수행하는 것이 필요
- ICO는 현행 데이터보호법과 GDPR 간의 주요 차이점을 해결하기 위해 이 체크리스트 및 ICO가 제공하는 기타 자료들을 활용하는 것이 중요하다고 강조

▶ 이 체크리스트는 기관/기업이 지금 당장 조치할 수 있는 12가지 단계를 설명

- 당장 조치 가능한 내용을 제시한 것은 기관/기업이 가능한 한 빨리 GDPR 준수를 위한 접근방식을 계획하고, GDPR의 투명성과 정보주체의 권리 관련 조항 등을 다루기 위한 새로운 절차를 마련하도록 하기 위함
- 기업이 GDPR이 규정하는 모든 영역을 준수하기 위해서는 데이터 보호 방식과 거버넌스에 대한 접근방식을 기업 차원의 이슈로 검토하는 것이 필요

2. 12가지 주요내용

① 인식(Awareness)

- 기존 법률이 GDPR로 대체될 것이라는 사실을 기관/기업의 의사 결정자들이 알고 있는지 확인하는 것 필요

1 이날 발표된 문서는 버전 1.1(Version 1.1)임

- 기관/기업의 지도부는 GDPR 체제 하에서 규정 준수 문제를 야기할 수 있는 영역들을 파악하고 그로 인해 예상되는 영향에 대해 제대로 인식할 수 있어야 함
- GDPR 발효 전까지 새로운 변화에 대해 준비를 하지 않으면 GDPR 규정 준수가 어려울 수 있다는 점에 대해서도 주의가 필요

② 보유하고 있는 정보(Information You Hold)

- 현재 '어떤 개인정보를 보유하고 있는가'를 포함해 해당 정보의 출처 및 정보를 공유하는 상대에 대해 문서로 기록하는 것이 필요
- 이와 관련해 조직 전체 또는 특정 비즈니스 영역 내에서 해당 사항을 파악할 수 있는 정보 감사(Information Audit)가 요구될 수 있음
- 부정확한 개인정보를 보유하고 이를 다른 조직과 공유한 경우에는, 해당 정보의 부정확성에 대해 그 조직에게도 통지하여 수정할 수 있도록 해야 하며, 이 같은 의무를 수행하기 위해서는 현재 보유 중인 개인정보가 무엇이며 누구와 공유했는가를 파악하는 것 필요
- 기관/기업은 GDPR의 책임성 원칙에 따라 정보보호를 위한 효과적인 정책 및 절차를 마련하는 등의 노력을 기울이고 있음을 보여주어야 하며, 관련 사항을 문서화해야함

③ 프라이버시 정보에 대한 커뮤니케이션(Communicating Privacy Information)

- 현행 개인정보보호 고지 방식을 검토하고 GDPR 시행에 따라 변경이 요구되는 경우 이에 대응하기 계획을 수립하는 것이 필요
- 개인정보를 수집할 때 현재는 '수집 주체가 누구'이며 '어떤 목적으로 사용할 것인가'에 대한 정보를 제공해야 하고, 이는 개인정보보호 고지(Notice)를 통해 이루어지지만, GDPR 체계 하에서는 정보주체에게 알려야 할 몇 가지 추가 사항이 있다는 점에 유의

  ※ ▲데이터 처리에 대한 법적 근거 ▲데이터 보유 기간 ▲정보주체가 자신의 데이터를 처리하는 방식에 문제가 있다고 생각하는 경우 ICO에 불만을 제기할 권리가 있다는 점을 알리는 것이 필요
- GDPR은 간결하고 이해하기 쉽고 명확한 언어로 이 같은 정보를 제공하도록 요구한다는 사실을 고려해 준비하는 것이 필요

④ 개인(정보주체)의 권리(Individuals' Rights)

- 개인정보 처리 절차[2]에서 정보주체의 모든 권리[3]를 보장하고 있는지 확인하는 것 필요

2 개인정보를 삭제하는 방식이나 데이터를 전자식으로(electronically) 혹은 일반적인 사용 형식으로 제공하는 방법 등을 포함

3 GDPR에 따른 개인의 주요 권리는 ▲데이터에 대한 정보주체의 접근(subject access), ▲부정확한 정보의 수정 ,▲잊힐 권리, ▲직접 마케팅 방지,▲자동화된 의사 결정 및 프로파일링 방지 ▲데이터 이동성(data portability) 보장 등을 포함

- GDPR 하에서 개인에게 보장된 권리는 전반적으로 영국의 현행 데이터보호법(DPA)의 권리와 주로 동일하지만, 몇 가지 중요한 개선 사항이 있으며, 현 시점에서 개인의 권리를 강화한다면 GDPR로 전환하는 과정이 비교적 더 쉬워질 것으로 기대

  ※ 정보주체가 자신의 개인정보를 삭제하도록 요청한 경우의 대처 방법에 대해 미리 준비한다면, 해당 데이터를 찾아내고 삭제하는 것이 가능한지 여부를 점검하고 누가 삭제에 대한 결정을 내릴 것인가를 결정하는 등 주요 문제에 대한 점검이 가능

- 데이터 이동성(Data Portability)에 대한 권리는 새로 도입되는 것으로서, 데이터를 인쇄물 형태 혹은 일반적으로 사용되지 않는 전자 형식으로 제공하는 조직의 경우에는 이번 기회를 계기로 관련 절차를 수정하고 필요한 사항을 변경할 것을 권고

⑤ 정보주체의 데이터 접근 요청(Subject Access Requests)

- 정보주체의 접근권(Right of access)을 보장하기 위해 ▲관련 절차를 업데이트 ▲시간 내에 해당 요청을 처리하는 방법을 계획▲추가 정보[4]를 제공하는 것이 필요
- 기관/기업은 정보주체의 요청을 준수하는 것에 대한 비용을 청구할 수 없고 통상적으로 현행 40일이 아닌 1개월 이내에 요청을 준수해야 할 전망
- 정보주체의 데이터 접근 요청을 거부할 수 있는 근거로는 분명하게 근거가 없거나 과도한 요청에 대해서는 데이터 접근에 따르는 비용을 부과하거나 요청을 거부하는 것이 가능
- 단, 요청을 거절하기 위해서는 해당 요청이 비용 부과나 거부 기준에 저촉되는 이유를 입증할 수 있는 방침과 절차를 마련해야 함
- 사람들이 온라인을 통해 정보에 쉽게 접근할 수 있는 시스템을 개발한다면 궁극적으로 상당한 관리 비용을 절감할 수 있을 것으로 기대되며, 이 같은 온라인 정보 접근 방식을 제공하는 것에 대한 비용/편익 분석을 수행할 것을 고려하도록 권고

⑥ 개인정보 처리를 위한 법적 근거(Legal Basis for Processing Personal Data)

- 현재 수행하고 있는 개인정보 처리의 다양한 유형을 점검하고, 해당 개인정보 처리를 수행하기 위한 법적 근거를 확인하여 문서화하는 것이 필요
- 예컨대, 개인정보 처리를 위한 법적 근거로서 '동의'를 사용하는 경우, 정보주체가 데이터 삭제를 요구할 수 있는 더 강력한 권한을 갖게됨
- 개인정보 취급방침을 제시할 때나 정보주체의 데이터 접근 요청에 응할 때는 개인정보 처리를 위한 법적 근거도 설명하는 것이 필요

4 정보주체는 GDPR에 규정된 접근권에 따라 일련의 정보를 취득할 권리를 보장받음. 즉, 정보주체는 본인에 관련된 개인정보의 처리 여부에 관련해 정보처리자로부터 확인을 획득할 권리를 가지며, 이 경우 개인정보 및 기타 규정된 정보에 대한 열람권을 갖는다 (GDPR 제15조 1항)

- GDPR이 인정하는 합법적인 개인정보 처리의 근거는 DPA의 법적 근거와 거의 동일하므로 조직이 수행하고 있는 다양한 개인정보 처리 유형을 검토하고 이에 대한 법적 근거를 확인하는 것이 가능해야 함

⑦ 동의(Consent)

- '동의' 방법을 찾고 동의를 확보하며 기록할 수 있는 방안을 점검하고 그것을 변경해야 하는지 여부에 대해 검토하는 것이 필요
- GDPR은 '동의'와 '명시적 동의(Explicit Consent)' 두 가지에 대해 언급하고 있으나, '동의'와 '명시적 동의' 모두 자유롭고, 구체적이며, 충분한 정보에 기초하여, 모호하지 않게 이루어져야 한다는 점을 고려할 때 둘 사이의 차이점은 명확하지 않음
- 또한 '동의'는 처리되는 개인정보에 대해 긍정적인 표시를 해야 성립되며, 정보주체가 침묵하거나 체크박스가 미리 채워져 있는 경우 또는 비활성화된 상태에서는 동의한 것으로 유추할 수 없음
- 따라서, 정보주체의 동의를 바탕으로 개인정보를 처리해야 하는 경우에는 GDPR에서 요구하는 표준을 충족하는지 확인해야 하며 충족하지 못하는 경우에는 동의 메커니즘을 변경하거나 동의를 대신할 수 있는 방안을 찾는 것이 필요
- 동의는 검증 가능해야 하며, 일반적으로 동의를 바탕으로 개인정보를 처리하는 경우에 정보주체들이 더 강력한 권한을 보유하게 된다는 점에 유의해야 함
- GDPR은 동의가 이루어졌음을 개인정보 처리자가 입증할 수 있어야한다는 점을 분명히 밝히고 있으므로, 감사(Audit) 과정에서 효과적인 상황 추적이 가능하도록 하기 위해 동의 사실에 대한 기록이 제대로 진행될 수 있는지 시스템을 점검할 것을 권고

⑧ 아동(Children)

- 정보주체의 연령을 확인하고 개인정보 처리 활동에 대한 부모 또는 보호자의 동의를 수집하기 위한 시스템을 구축하는 것에 대해 고려하는 것이 필요
- GDPR은 특히 SNS와 같은 상업적 인터넷 서비스의 맥락에서 아동의 개인정보보호 문제에 각별한 관심을 표하고 있음
- 영국에서는 13세 미만의 개인을 아동으로 정의하므로, 이들의 개인정보를 합법적으로 처리하기 위해서는 부모 또는 보호자의 동의가 필요
- 아동 대상의 서비스를 목표로 개인정보를 수집하는 경우, 동의는 입증될 수 있어야 하고 아동의 개인정보를 수집할 때 개인정보보호에 관한 고지는 아동이 충분히 이해할 수 있는 언어로 작성되어야 한다는 것을 반드시 기억해야 함

⑨ 정보 유출(Data Breaches)

- 개인정보 유출을 탐지·보고·조사할 수 있는 올바른 절차를 마련하는 것이 필요
- 일부 조직의 경우 개인정보 유출 사고가 발생했을 때 ICO에 통보하는 것이 이미 의무화되어 있으나, GDPR에 따라 이 같은 사고 통지 의무가 전체로 확대될 것이며 많은 조직들이 이러한 상황에 처음 노출되는 상황
- 단, 모든 개인정보 침해 사실이 ICO에 통보되어야 하는 것은 아니며, 신분 도용 또는 기밀 유출과 같은 특정 형태의 손해가 발생할 수 있는 경우에만 해당
- 조직들이 개인정보 유출을 탐지·보고·조사할 수 있는 절차를 마련하는 것과 관련해서는 ▲보유한 데이터의 유형을 평가하고 ▲개인정보 침해 사항이 발생한 경우 통지 요건에 해당하는 데이터를 문서화하는 것 등이 포함
- 경우에 따라서는 직접적인 정보유출 피해가 발생한 개인에게 그 사실을 통보해야 하며, 예컨대 개인정보 침해로 인해 재정적 손실의 위험에 노출된 경우 등이 이에 해당
- 상대적으로 규모가 큰 조직은 중앙 또는 지역 차원에서 정보 유출을 관리하기 위한 정책 및 절차를 개발해야 하며, 유출 사실을 신고해야하는 경우임에도 불구하고 보고가 이루어지지 않은 경우에는 정보 유출사고 그 자체에 대한 과징금 이외에 보고 의무 태만에 대한 별도의 과징금이 부과될 수 있음

⑩ 정보 보호 중심 디자인과 정보보호영향평가
(Data Protection by Design and Data Protection Impact Assessments)

- ICO가 개인정보영향평가(이하 'PIA')에 대해 작성한 지침을 숙지하고, 이를 조직에 구현할 방법에 대해 준비하는 것이 필요
- 이 지침은 PIA가 조직 내 다른 프로세스와 어떻게 연계될 수 있는지 보여주며, PIA(GDPR의 용어로는 DPIA)가 반드시 수행되어야 할 상황에 대해 평가하는 것부터 시작하는 것이 바람직
  ※ 다음과 같은 질문이 필요: ▲누가 담당할 것인가? ▲그 밖에 누가 더 관여해야 하는가? ▲해당 프로세스는 중앙과 로컬 중 어디에서 실행되어야 하는가?
- 항상 PIA를 수행할 필요는 없으며, PIA는 새로운 기술이 배치되거나 프로파일링 작업이 개인에게 중대한 영향을 줄 수 있는 경우와 같이 리스크가 높은 상황에서 필요함
- PIA 결과 데이터 처리 과정에서 위험성이 높은 것으로 나타난 경우, 해당 처리 작업이 GDPR을 준수하는지 여부에 대해 ICO와 상의하고 의견을 구하는 것이 필요

⑪ 정보보호책임자(Data Protection Officers, DPO)

- 필요한 경우, 정보보호책임자(DPO) 또는 정보보호 컴플라이언스 업무 책임자를 지정하고 이 역할을 어떤 위치에 두어야 조직의 구조 및 거버넌스와 조화를 이룰 수 있는지 평가해야 함

- GDPR로 인해 일부 조직(예: 공공기관 또는 대규모로 정보주체들에 대한 정기적이고 체계적인 모니터링 관련 활동에 종사하는 조직)들에 대해 정보보호책임자(DPO) 지정이 의무화될 것
- 이 때 조직 내부 구성원 혹은 외부의 정보보호 담당 고문이 정보보호 규정 준수에 대한 적절한 책임을 지고 이를 효과적으로 수행할 수 있는 지식 및 권한을 가지고 있는지 확인하는 것이 중요
- 따라서, 정보보호책임자를 지정해야 하는 대상인지 여부를 고려하고, 현행 정보보호 컴플라이언스 접근 방식이 GDPR의 요구사항을 충족하는지 여부에 대해 평가하는 것 필요

⑫ 국제 관련 이슈들(International)

- 국제적으로 운영되는 조직의 경우 어떤 국가의 정보보호 감독기관을 관할로 할 것인지 결정하는 것이 필요
- 해당 조직의 데이터 처리에 대한 결정이 어디에서 이루어지는가에 따라 해당 사안에 대한 주관 정보보호감독 당국이 결정됨
- 그러나 데이터 처리가 서로 다른 장소에서 이루어지는 복잡한 다중 지역(Multi-site) 조직의 경우에는 문제가 어려워질 수 있으며, 관할 감독 당국을 결정하기가 모호한 경우에는 데이터 처리에 관한 가장 중요한 결정을 내리는 곳을 파악하는 것이 도움이 될 수 있음

<그림1> ICO가 제시하는 'GDPR 시행에 대비한 12가지 조치사항'

3. ICO의 향후계획

▶ GDPR 실행을 앞두고 향후 수개월 동안 ICO는 GDPR 대응을 위한 위한 새로운 지침[5] 및 기타 툴(Tools)을 마련할 계획이며, 29조 작업반 또한 유럽 차원에서 지침을 제정할 예정

- 또한 ICO는 여러 산업 부문을 대표하는 무역 협회 및 각종 기관들과 긴밀히 협력할 예정
- GDPR의 시행을 준비하며 ICO의 업무는 더욱 강화될 것으로 예상
- 엘리자베스 덴햄(Elizabeth Denham) 위원장은 ICO의 역량 강화를 위해 인원을 증원하고 전문성을 향상시키기 위한 프로그램을 준비할 계획

Reference

1. ICO, Preparing for the General Data Protection Regulation(GDPR): 12 steps to take now, 2017.3.13
2. ICO, ICO releases annual performance statistics for 2016/17, 2017.6.12
3. Personnel Today, ICO opens consultation on consent under the GDPR, 2017.3.6

5 예컨대 ICO는 GDPR의 개인정보 동의요건과 관련, 2017년 3월 31일까지 지침서 초안(Draft Guidance)에 대한 의견검토를 진행한 바 있음. 이 지침서 초안은 △GDPR 체제 하에서 개인정보 처리에 관한 동의가 적절한 때는 언제이며, △유효한 동의의 요소가 무엇이고, △동의를 확보한 후 이를 어떻게 관리해야 하는가에 대한 내용을 설명

KISA 한국인터넷진흥원

발 행 일 2017년 5월
발 행 및 편 집 한국인터넷진흥원 개인정보보호본부 개인정보기획팀
주 소 서울시 송파구 중대로 135(가락동 78) IT벤처타워 Tel 02.405.5118