2024. 7. 17.(수) 14:00
정부서울청사 3층 브리핑룸

『AI 개발·서비스를 위한 공개된 개인정보 처리 안내서』

Q&A

개인정보보호위원회

1. 안내서가 적용되는 '공개된 개인정보'가 무엇인지?

□ 본 안내서의 대상인 '공개된 개인정보'는 **누구나 합법적으로 접근 가능**한 개인정보로서,

○ 주로 웹사이트, 블로그, 위키백과, 커먼크롤, 법령에 의해 공시·공개된 개인정보, 출판물, 방송매체 등에 포함된 개인정보 등을 의미

○ **비공개** 또는 **일부에게만 공개된 정보**, **사인간의 대화** 등은 공개된 개인정보에 **해당하지 않음**

□ 현재 많은 국내외 **AI 기업** 등이 **학습데이터 확보**를 위하여 **웹 스크래핑** 등을 통해 공개적으로 접근 가능한 데이터를 수집하여 활용하고 있음

2. 실수로 카드번호, 고유식별번호 등 민감한 정보를 공개했을 수 있는데, 이러한 정보가 활용되면 문제가 생기지 않는지?

□ 공개된 데이터에는 **위법**하거나 **실수로 공개된 개인정보**가 포함되어 있을 수 있어서 **일정한 안전조치가 필요함**

□ **개인정보위와 KISA**는 공공·민간홈페이지를 대상으로 주민등록번호, 여권번호, 운전면허 번호 등 **보호법상 노출이 금지된 개인정보**의 노출 및 불법적 유통을 **탐지하여 삭제**하고 있으며,

○ **탐지된 사이트의 URL**를 주기적으로 업데이트하여 **AI 기업 등에게 공개**하고 있는데, 기업은 해당 사이트를 **학습 데이터에서 배제**하여 안전성을 높일 수 있음

□ 아울러, 「**안내서**」에서 민감한 정보가 노출되지 않도록 하기 위한 **안전성 확보조치*를 안내**했으니 기업들은 **상황에 맞춰 적용**할 수 있음

* △특정인 개인정보를 묻는 질문에 답변하지 않도록 하는 등 프롬프트 필터링 적용, △고유식별정보 등 민감한 정보는 사전 비식별화 등

3. 기업 입장에서는 안내서에 제시된 여러 안전조치를 도입해야 한다는 부담을 느낄 수 있는데, 이에 대한 개인정보위 입장은?

□ 기업에게 본 안내서에서 제시된 **모든 안전조치의 도입과 이행이 요구되는 것은 아님**(안내서에도 명시함)

○ 기업이 AI 유형, 용례 등 **개별 여건에 따라** AI 성능과 안전성의 조화를 이룰 수 있는 **최적의 안전성 확보 조치를 자율적으로 도입**할 수 있도록 안내하여 **일률적인 규제로 인한 부담은 없도록 함**

□ 또한, 안내서는 AI 학습에 공개된 개인정보를 수집·활용할 수 있는 **기준·요건을 명확히 안내**하였기에 **기업 부담이 줄어드는 측면**도 있을 것임

○ 생성형 AI를 개발하는 **주요 기업**들은 **이미 일정한 안전조치를 시행 중**이지만, 안내서를 통해 기업·학계에서 연구되고 있는 **다양한 안전조치를 안내**받음으로써 기존의 개인정보 **보호조치를 재점검하고 보완**하는 데에 참고할 수 있을 것임

4. 「안내서」에 열거된 안전성 확보조치 및 정보주체 권리보장 방안을 미이행하면 AI 기업에 어떤 불이익이 있는지?

□ 본 안내서에서 제시하는 **개별 조치를 이행하지 않았다고 하여** 공개된 개인정보 처리가 곧바로 **위법한 것은 아님**

○ 다만, 사업자가 **예상할 수 있거나 실존하는 리스크**에 대하여 **적절한 안전조치를 취하지 않는 것이 원인이 되어** 중대한 **정보주체 권리침해**가 발생하는 경우,

○ **'정당한 이익'**을 공개된 개인정보 처리의 법적 근거로 주장하는 **타당성이 인정되지 못할 수 있음**

□ **안내서의 목적**이 조사나 제재가 아니라 **AI 기업 등의 불확실성 해소**에 있는 만큼,

○ 안내서 발간 이후에 주**요 AI 기업과 소통**하면서 AI 안전성 확보를 위한 **기업의 조치를 모니터링**하고 개인정보가 안전하게 활용될 수 있는 여건을 조성하기 위한 **정책적 노력을 지속**해 나가겠음

5. AI 기업이 정당한 이익을 근거로 공개된 개인정보를 처리하면, 이를 기업이 입증해야 하는지?

□ 공개된 개인정보 처리의 적법성에 대한 **입증 책임은 원칙적으로 기업이 부담**함

○ 정당한 이익을 원용하는 AI 기업은 안내서에 제시된 판단기준 및 적용사례를 참고하여 **적법근거 충족 여부를 자율적으로 평가**하고 **그 근거를 문서화**하는 것이 권장됨

6. 기업이 자율적으로 안전조치의 최적조합을 검토·도입하라는 것이 오히려 기업 입장에서는 규제 불확실성이 커지는 것 아닌지?

□ AI는 **기술·서비스 구조, 적용 분야, 목적 등이 다양**하고, 발전 양상이 매우 변화무쌍한 기술임

○ 현재 AI의 성능을 발전시키면서도 공정성, 투명성, 안전성 등을 높일 수 있도록 **다양한 조치들이 논의**되고 있으나, 아직까지 **'만능 해결책'으로서의 안전조치는 알려진 바 없음**

○ 안전성을 높일 수 있는 개별 조치는 **편향·차별, 성능 저하 등의 부정적 효과**를 야기할 수 있어, 특정 안전조치 이행을 일률적으로 요구하기 보다는 **기업 자율로 「최적 조합」을 선택하여 이행**하도록 함

□ 단, 기업 입장에서는 「최적 조합」 판단에 불확실성이 있을 수 있으므로,

○ 이번 안내서에 **실제 기업들의 사례를 소개**했고, 향후에도 AI 기업이 참고할 수 있도록 업계에서 연구·시행되고 있는 **모범사례를 지속적으로 발굴**하여 **안내서에 반영**할 계획임

7. 안내서로 인하여 국내 기업과 글로벌 기업 간에 차별이 발생할 우려는 없는지?

□ 동 안내서는 **국내외 사업자에게 동일하게 적용**되므로 안내서로 인한 국내외 **기업간 차별 우려는 없음**

○ 또한, 안내서 마련 과정에서 **국내외 기업과 수시로 소통**하면서 의견을 청취하고 안내서에 반영하였음

< 안내서 적용 대상 해외사업자 >

① 해외사업자가 한국 정보주체를 대상으로 재화·서비스를 제공하는 경우

② 한국 정보주체를 대상으로 재화 또는 서비스를 제공하지 않더라도 한국 정보주체의 개인정보를 처리하여, 직접적이고 상당한 영향을 미치는 경우

※「해외사업자의 개인정보 보호법 적용 안내서」참고

8. 다른 경우에도 '정당한 이익' 조항을 근거로 개인정보 활용을 인정한 사례가 있는지?

□ 그간 국내 정당한 이익 조항은 **제한적으로 적용**되어 왔고, 아직까지 관련 판례나 위원회 결정 **사례는 많지 않음**

○ 기존 사례를 보면, **다양한 안전조치**를 통해 사생활 침해 우려를 낮춘 경우 **정당한 이익이 인정**되었음

○ 안내서는 AI 개발·서비스에 한하여 '정당한 이익' 조항을 적용하는 기준으로서, 기존 사례와 **비슷한 맥락**에서 **충분한 안전조치를 전제**로 AI 사업자의 정당한 이익이 인정될 수 있는 **3가지 요건을 제시함**

9. 공개된 개인정보로 학습된 AI가 특정인을 식별하는 목적으로 사용되거나, 범죄 등에 악용되는 것은 아닌지?

□ **개인식별 목적**으로 사용되어 **범죄 등에 악용**되는 AI의 경우에는 **'정보주체의 권리'**에 **우선**해야만 성립될 수 있는 **'정당한 이익'**이 원칙적으로 **성립될 수 없음**

○ 안내서에도 ①**안면인식 DB**와 결합하여 개인에 대한 **프로파일링 및 감시** 목적의 AI 개발, ②**사이버 공격**이나 **피싱·스미싱** 등 개인 사칭 사기 목적의 AI는 **목적의 정당성이 인정될 수 없다고 안내**함

□ 참고로, 공개된 개인정보를 학습하여 **오픈소스로 공개**된 AI 모델의 악용 가능성을 방지하기 위해, 여러 AI 기업에서는 **안전하고 책임있는 AI 사용을 위한 라이선스 정책**을 마련·시행하고 있음

○ **AI 개발자-배포자-이용사업자** 등 간의 **책임분담**과 **역할**에 대해서는 **추가적인 검토**가 필요한 사항임