

요약

EIOPA의 설문조사에 따르면, 다수의 유럽 보험회사가 생성형 AI 모델에 자사 데이터를 학습시켜 업무 효율을 높이고 있음. AI 확산에 따라 새로운 유형의 리스크가 부각되면서, 보험회사들은 이에 대응하기 위한 대응 체계와 통제 장치를 정비하고 있음. EIOPA는 인공지능법이 보험업계에 미치는 영향을 평가하는 한편, 투명한 데이터 활용과 소비자보호 강화를 위한 감독지침을 고도화할 계획임

- 유럽보험연금감독청(EIOPA)에 따르면 유럽의 보험회사들이 생성형 AI를 활용하고 있으며 보험업계에서 AI 활용 범위가 클 것으로 예상됨¹⁾
 - EIOPA는 2025년에 25개의 유럽연합(EU) 및 유럽경제지역(EEA) 회원국에 속한 347개 생명보험회사 및 손해보험회사를 대상으로 설문조사를 시행함
 - 설문조사 결과, 유럽 보험회사의 65%가 생성형 AI를 실무에 활용 중이며 23%가 3년 내 도입을 계획하고 있음
- 보험회사들은 주로 외부에서 구입한 생성형 AI 모델에 자사 데이터를 학습시켜서 실무에 활용하여 보험산업 가치사슬 전반의 효율성을 증대시키고 비용을 절감하는 등 긍정적인 효과를 창출함
 - 자체 모델을 개발하면 막대한 비용이 들기 때문에 외부 상용 모델을 구매하거나 외부 모델에 자사의 언더라이팅 가이드라인을 결합하는 하이브리드전략을 채택하는 것으로 보임
 - 프랑스 보험회사인 AXA는 OpenAI의 모델을 구매한 후 자사의 보험약관, 고유의 업무방식 등의 데이터를 입력하여 AXA 전용 생성형 AI인 AXA Secure GPT를 개발함²⁾
 - 생성형 AI의 데이터 학습 방식으로 자사의 내부 데이터를 모델에 연결하면서도 비용과 AI의 환각(Hallucination) 오류를 줄일 수 있는 검색 증강 생성(RAG)³⁾ 기술이 가장 선호되고 있음
 - 생성형 AI는 언더라이팅과 후선업무 지원 부서의 생산성을 높이고, 보험금 지급 과정에서는 고객문의에 신속하게 응대하는 챗봇으로서 전반적인 고객서비스를 개선하고 있음
- 생성형 AI로 인한 리스크를 통제하기 위해 리스크 관리의 초점이 기존 모델 학습 단계에서 벗어나 사용자의 프롬프트 설계 및 산출물을 검증하는 추론 방식으로 변화함

1) EIOPA(2025. 2. 1.), "Generative AI Market Survey: Outlook, Use Cases and Risk Management"

2) AXA(2024. 4. 24.), "AXA harnesses the power of secure generative AI with Azure OpenAI Service"

3) RAG(Retrieval-Augmented Generation)란 사전 학습된 AI 모델을 외부 지식 데이터베이스에 연결하는 기술적 접근법을 뜻하며, 시스템이 먼저 관련성 있고 검증 가능한 정보를 검색한 뒤, 그 문맥적 정보를 사용자의 프롬프트에 추가하는 형태로 작동함

- 과거에는 기업이 AI에 자사 데이터를 직접 학습시켰으나, 생성형 AI는 외부의 데이터를 사전 학습하여 데이터 학습 방식에 대한 직접적인 통제가 어렵기에 산출물 출력 방식에 관한 리스크 관리가 중요해짐
- 생성형 AI의 도입으로 신종 사이버 보안 공격, AI 환각(Hallucination) 등이 새로운 리스크 요인으로 부상함
- 유럽 보험회사의 49%가 AI 전담 내부 정책을 마련하였으며, IT·법무 등 여러 부서가 결합된 AI 리스크 관리 위원회를 구성해 기술적 통제 장치와 전사적 대응 체계를 구축하고 있음(〈표 1〉 참조)

〈표 1〉 리스크 유형에 따른 기술적 통제 장치 및 전사적 대응 체계

리스크 유형	통제 장치 및 대응 체계	리스크 통제 및 대응 방법 설명
환각	동일한 질문을 미세하게 변경해 반복 입력함으로써 산출물의 일관성이 없을 시 경고를 발생시키는 안전장치 설계	결과물 출력 과정의 투명성 향상
사이버 보안	프롬프트 인젝션 ¹⁾ 방어, 프롬프트 암호화	LLM 특유의 비결정적 출력 변동성 관리
데이터 보호	데이터 익명화, 샌드박스 테스트 ²⁾	개인의 기본권 침해 여부를 평가하는 기본권 영향 평가 실시
설명 가능성 부족	프롬프트 엔지니어링 ³⁾ 기록 문서화, 단계별 의사결정 추적	인적 감독 활성화 및 인간의 최종 검증
제3자 의존성	DORA ⁴⁾ 준수, 계약상 책임 명시, 공급망 리스크 감사	기술 제공자의 책임 소재 명확화

주: 1) 공격자가 조작된 프롬프트를 입력해 모델에 내장된 안전장치를 무력화시키고 기밀정보를 유출하는 행동 등의 신종 사이버 보안 공격임

2) 실제 운영환경에 영향을 주지 않고, 격리된 가상공간에서 소프트웨어, 앱, 결제 시스템 등을 안전하게 검증하는 방식임

3) 생성형 AI가 사용자가 입력하는 텍스트 기반의 지시어(프롬프트)를 구조화하고 수정 및 개선하는 일련의 과정임

4) DORA(Digital Operational Resilience Act)는 AI 제공업체와의 계약상 합의를 포함하여 기업의 ICT(정보통신기술) 리스크 관리에 대한 상세한 규정을 담고 있는 법안임

자료: EIOPA(2025. 2. 1.), "Generative AI Market Survey: Outlook, Use Cases and Risk Management"

○ 인공지능법은 AI 시스템의 제공자, 배포자, 수입자 등 다양한 이해관계자에게 AI 특화 리스크 관리 의무를 부여하고 있으며, EIOPA는 인공지능법이 보험업계에 미치는 영향을 모니터링하며 감독 지침을 고도화할 계획임

- 유럽 보험회사들은 생성형 AI 활용 시 빅테크 등 외부 클라우드 제공업체에 대한 의존도가 높는데, AI 제공업체들은 영업 비밀을 이유로 AI 모델의 구체적인 설계 방식이나 학습 데이터의 출처를 투명하게 공개하지 않기에 단순 보안 인증을 확인하는 감사와 같은 기존의 규제 방법은 한계가 있음
- 새로 도입된 EU의 인공지능법은 공동 책임 방식을 채택하여 AI를 활용하는 보험회사뿐만 아니라 공급자인 AI 제공업체에도 투명성, 문서화 및 리스크 관리 의무를 부과함
 - 구글은 Munich Re와 협력하여 구글 클라우드 고객 전용 맞춤형 사이버 보험상품을 출시하였으며, 이를 통해 자체 클라우드 서비스에서 발생한 사이버 사고로 인한 재무적 손실 리스크를 포괄적으로 보호하고 있음⁴⁾
- EIOPA는 새로운 규제 환경하에서 AI 제공자 및 배포자에게 부여되는 투명성과 리스크 관리 의무의 실질적 파급 효과를 평가하고, 국제보험감독자협의회(IAIS)와 협력하여 글로벌 감독기준을 수립할 계획임
 - 건전한 데이터 활용을 위해 '데이터 활용 자문 전문가 그룹'을 신설하여 2026년 2분기까지 관련 보고서를 발간할 예정이며, 취약 계층 소비자에 대한 공정한 대우를 위해 리스크 주제별 심층 검토 작업을 추진하고 있음

4) Munich Re(2026), "Cloud Protection+ Innovative Cyber Insurance Solution exclusively for Google Cloud Customers"