

에이전틱 인공지능(Agentic AI)과 개인정보보호, 민관 협력을 통한 합리적 규율체계 모색

- 「인공지능 프라이버시 민·관 정책협의회(2기)」 제2차 전체회의 개최
- 에이전틱 인공지능 프라이버시 이슈와 개인정보 제도 혁신 방향 논의

개인정보보호위원회(위원장 송경희, 이하 ‘개인정보위’)는 9월 23일(수) 오후 은행회관 국제회의실에서 「인공지능(AI) 프라이버시 민·관 정책협의회(2기) 제2차 전체회의」를 개최했다.

인공지능 프라이버시 민·관 정책협의회(‘23.10~)는 인공지능 시대 변화하는 개인정보 처리환경에서 활용과 보호가 조화를 이룰 수 있도록 합리적 규율 방향을 설계하는 민관 협력체계다. 올해 2월, 에이전틱 인공지능(Agentic AI) 등 새로운 기술환경에 대응하여 정책협의회 2기*를 출범했다.

* (의장) 송경희 개인정보보호위원장, 권창환 수원지방법원 부장판사, (위원) 학계, 산업계, 법조계, 시민단체 등 36명, (구성) 1분과(데이터 처리기준), 2분과(리스크 관리), 3분과(정보주체 권리보장)

이번 전체회의는 두 개의 주제 발표와 종합 토의로 진행했다.

먼저 김병필 카이스트(KAIST) 교수가 ‘에이전틱 인공지능의 프라이버시 이슈’를 주제로 발표했다. 발표에서는 1분과 활동의 일환으로 진행된 현장 인터뷰(2026.7월~8월) 주요 결과와 향후 검토 과제를 제시했다. 인터뷰는 국내외 인공지능 개발·도입 기관 15곳을 대상으로 진행했으며, 현장의 에이전틱 인공지능 활용 사례, 개인정보 보호 측면의 위험 요인, 법적 불확실성 등을 파악하기 위해 실시됐다. 인터뷰 참여 기관들은 프롬프트 인젝션*(Prompt injection), 에이전틱 인공지능에 부여되는 과도한 권한 등을 주요 위험요인으로 꼽았다. 아울러 ▲자율·승인 경계 설정, ▲참여 주체별 지위와 책임, ▲로그·메모리 등의 개인정보 보관·파기 등에 대한 기준이 필요하다는 의견을 제시했다. 향후 마련될 안내서는 원칙·위험 기반의 접근과 기술 중립성을 견지할 필요가 있다는 의견도 제시됐다.

* 인공지능의 입력에 악의적인 명령어를 주입하여 시스템이 의도하지 않은 동작을 수행하도록 유도하는 공격 기법

이어서 최윤정 개인정보보호정책과장이 ‘인공지능 시대 개인정보 제도 혁신 방향’을 소개했다. 데이터 처리 방식이 빠르게 변화하면서 현행 개인정보 보호체계도 새로운 환경에 맞게 정비할 필요성이 커지고 있다. 이에 따라, 국민의 권리보호에 미치는 영향은 적으면서 데이터 활용을 제약하는 형식적인 규제는 합리적으로 개선하고, 인공지능 시대에 필요한 규범은 신속히 마련할 예정이다.

이어진 종합 토의에서는 인공지능 데이터 확보·활용을 위한 처리근거 유연화, 인공지능 개인정보 활용 특례*의 합리적 운영, 인공지능 환경에 적합한 실질적인 안전장치 및 책임구조 마련 등을 중심으로 다양한 의견이 제시됐다. 논의 결과는 개인정보위가 올해 말 공개 예정인 「가칭에이전틱 인공지능 개인정보 처리 안내서」 및 제도 혁신방안에 반영될 예정이다.

* 가명·익명정보만으로는 인공지능 개발이 곤란하고, 공익·사회적 필요성이 인정되는 경우, 강화된 안전조치와 개인정보위의 심의·의결을 전제로 적법하게 수집한 개인정보를 인공지능 기술개발에 활용할 수 있도록 허용(『개인정보 보호법』 개정안 '27.3.9. 시행)

송경희 개인정보위 위원장은 “국민 편익을 가져오는 기술 발전은 충분히 뒷받침하면서 국민의 프라이버시 보호를 비롯한 권리와 안전을 함께 지켜나가야 기술이 지속 가능할 수 있다.”라며, “민관이 협력하여 합리적이고 균형 잡힌 인공지능 개인정보 규율체계를 마련해 나가겠다.”라고 말했다.

권창환 공동의장은 “스스로 과업을 수행하는 에이전틱 인공지능은 개인정보의 영역에서도 새로운 과제를 제기하고 있다.”라며, “이러한 시기에 산업 현장의 목소리를 정부에 충실히 전달하고 민관이 함께 합리적인 규율 방안을 모색함으로써 사업자의 책임 있는 혁신과 정보주체의 실효적인 권리 보호가 조화를 이룰 수 있게 되기를 기대한다.”라고 말했다.

담당 부서 <총괄>	개인정보정책국 인공지능프라이버시팀	책임자	팀 장	주문호 (02-2100-3073)
		담당자	사무관	임수연 (02-2100-3078)
			주무관	박은지 (02-2100-3169)
담당 부서	개인정보정책국 개인정보보호정책과	책임자	과 장	최윤정 (02-2100-3051)
		담당자	사무관	이정수 (02-2100-3052)
관련 기관	한국인터넷진흥원 AI데이터정책팀	책임자	팀 장	박상준 (061-820-2990)
		담당자	주 임	배우리 (061-820-2993)

□ 개요(안)

- (목적) 「AI 프라이버시 민·관 정책협의회」 2기 출범(‘26.2.2.) 이후
분과별* 진행사항 및 향후 계획 공유, 주요 정책 의견수렴
- * (1분과) 데이터 처리기준, (2분과) 리스크 관리, (3분과) 정보주체 권리보장
- (일시/장소) 9.23.(수) 15:00~17:00 / 은행회관 국제회의실(2층)
- (참석자) 개인정보위 위원장·사무처장·정책국장, 과기정통부, 행안부,
방미통위, AI 프라이버시 민·관 정책협의회 위원(학계, 법조계, 산업계,
시민단체), KISA 등 약 40명
- (주요내용) <1부> AI 프라이버시 주요 현안 발제 및 <2부> 분과별 진행
상황 공유 등 종합 라운드테이블을 통한 정책 의견수렴

□ 세부계획

※ 발제1까지 언론 공개

시간		행사 내용	비 고
1 부	15:00~15:02	개회 및 회의 안내(2')	사회: AI프라이버시팀장
	15:02~15:07	인사말씀(5')	송경희 위원장, 권창환 공동의장
	15:07~15:10	사진촬영(3')	참석자 전체
	15:10~15:25	발제1. 에이전틱 AI의 프라이버시 이슈(15')	KAIST 김병필 교수
	15:25~15:40	발제2. ^{가칭} AI 시대 개인정보 제도 혁신 방향(15')	개인정보정책과장
자리 정돈 및 휴식시간(10')			
2 부	15:50~16:55	종합 라운드테이블(65')*	사회: 권창환 공동의장
		- ① 분과별 추진현황 및 향후과제 발표(10')	분과장
		- ② 발제 안건 관련 자유토론(10')	분과장·정책국장
		- ③ 자유 질의 및 제언(45')	참석자 전체
	16:55~17:00	마무리 말씀 및 폐회(3')	개인정보위원장

* 패널 : 김병필 교수(1분과장), 최대선 교수(2분과장), 홍준호 교수(3분과장 대리), 이상민 정책국장