

# 2025년 데이터프라이버시 연구회 제 3회 워크샵 “AI 기술에서 개인정보는?”

**일 자** 2025년 04월 24일(목) ~ 04월 26일(토)  
**장 소** 강원도 홍천 비발디파크 소노벨 C동 크리스탈볼룸  
**진 행** 온 · 오프라인 병행  
**주 최** 한국정보처리학회  
**주 관** 데이터프라이버시 연구회  
<https://sigdp.kips.or.kr>

## 초대의 글

안녕하십니까.  
 한국정보처리학회에서 주최하는 데이터프라이버시 연구회 워크샵에 여러분을 초대합니다.  
 현대에서 살고 있는 우리들은 인터넷과 단절되어서는 살기 어려운 세상에서 살고 있으며, 인터넷에서 제공되는 다양한 서비스는 우리의 생활을 더욱 편리하게 만들고 있습니다. 하지만, 이러한 편리함의 이면에는 인터넷 사용자에 대한 개인정보의 수집과 활용에 대한 이슈가 큰 문제점으로 제기되고 있습니다. 한국정보처리학회 데이터프라이버시 연구회에서는 산학연 전문가들을 모시고 이러한 개인정보보호 관련된 연구 및 이슈를 논의하고자 "AI 기술에서 개인정보는?"이라는 제목으로 워크샵을 개최하오니 많은 관심과 참여 부탁드립니다.  
 데이터프라이버시 연구회 위원장 한양대학교 임을규 올림.

2025. 4

데이터프라이버시 연구회 위원장 **임을규**

## 준비 위원

조직위원장	임을규 교수(한양대)			
프로그램위원	강유성 실장(ETRI) 이준 센터장(KISTI)	권태경 교수(서울대) 심동욱 단장(KISA)	박하은 교수(경희대)	이용우 박사(연세대)
운영위원	강병훈 교수(KAIST) 김진욱 위원(개인정보보호위원회) 박기웅 교수(세종대) 심동욱 단장(KISA) 조성제 교수(단국대)	권태경 교수(서울대) 방혁준 대표(쿠팡) 안용대 교수(송실대) 조영필 교수(한양대)	김성현 수석(NIA) 김창희 실장(안랩) 백윤홍 교수(서울대) 이혁기 박사(디사일로) 조지훈 마스터(삼성SDS)	김정여 본부장(ETRI) 류승진 실장(NSR) 송중석 본부장(KISTI) 정은수 교수(청주대) 채상미 교수(이화여대)

## 프로그램

04월 24일(목)	행 사 내 용
장 소	SONO BELLE Tower C 1층 라일락 I
세션명	튜토리얼 좌장: 김기범 본부장 (NSR)
15:00~16:00	LLM RAG (Retrieval-Augmented Generation) 오현영 교수(가천대학교) 좌장: 김정여 본부장 (ETRI)
16:00~17:00	동형암호 컴파일러 이용우 박사(연세대학교)
18:00~	Welcome reception (Only for Invited Members)
04월 25일(금)	행 사 내 용
장 소	SONO BELLE Tower C 1층 크리스탈 볼룸
세션명	프라이버시 보호 기술 좌장: 조영필 교수 (한양대)
09:00~09:40	Summation-based Private Segmented Membership Test from Threshold-Fully Homomorphic Encryption (Online 발표) 정태호 교수(Univ. of Norte Dame)
09:40~10:20	MPC기반의 얼굴바이오 분산 인증 기술 조관태 책임(ETRI)
10:20~11:00	대규모 언어 모델(LLM)의 위협과 이용자 권리보호 방안 장재영 박사(한국인터넷진흥원)
세션명	합성 데이터 좌장: 강유성 실장 (ETRI)
11:00~11:40	데이터 합성 최신 기술동향과 도전적 이슈 임중호 교수(연세대학교)
11:40~12:20	합성데이터 안전성 및 유용성 평가 김승환 교수(인하대학교)
12:20~13:30	중 식
세션명	초청 강연 좌장: 백윤홍 교수 (서울대)
13:30~14:20	AI 안전에서의 개인정보보호 김명주 소장(AI 안전 연구소)
14:20~14:30	휴 식
세션명	프라이버시 이슈 사례 좌장: 송중석 본부장 (KISTI)
14:30~15:10	고객사의 다양한 개인정보보호 이슈 정창모 박사(달로이트 컨설팅)
15:10~15:50	의료AI 학습시 의료데이터 활용 규제의 문제점 구태연 변호사(법무법인 린)
15:50~16:00	휴 식
세션명	LLM 보안 위협 좌장: 조병선 차장 (한전KDN)
16:00~16:40	딥시크 보안 취약점(인젝션 및 제일브레이크 중심) 윤두식 대표(이로운앤컴퍼니)
16:40~17:20	Trustworthy LLM: Jailbreaking and Fairness 이우진 교수(동국대학교)
17:20~18:00	변화의 중심, LLM 기반 에이전트: 새로운 보안 위협과 대응 전략 송현민 교수(단국대학교)
18:30~	만찬
04월 26일(토)	행 사 내 용
장 소	SONO BELLE Tower C 1층 라일락 I
10:00~13:00	Social Events & Post Workshop Meeting (Only for Invited Members)

## 등록 안내

📍 사전등록기간 : ~ 2025년 04월 23일(수) 자정

등록비	구분	사전등록	현장등록
	일반	450,000원	500,000원
	학생	250,000원	300,000원

\*온·오프라인 동일합니다.

📍 등록방법

- 한국보처리학회 홈페이지 접속 (<https://www.kips.or.kr>)
- (학회 공지/행사) ▶ 본 행사 선택 ▶ 사전등록 바로가기 후 등록 정보 작성 및 결제 진행

📍 등록관련문의

- 한국정보처리학회 ☎ 02-2077-1414, 내선 3번, [ysyun@kips.or.kr](mailto:ysyun@kips.or.kr)

📍 참가 증명서 발급

- 데이터프라이버시 연구회 간사, [ypcho@hanyang.ac.kr](mailto:ypcho@hanyang.ac.kr)

📍 오시는 길

- 비발디 파크, 크리스탈볼룸 & 라일락 I
- 주소 : 강원특별자치도 홍천군 서면 한치골길 262
- 택시 이용 : 홍천 터미널 약 35분 소요