2024 Vol.10

PRIVACY REPORT

개인정보보호
월간동향분석

2024년 10월호

KISA 한국인터넷진흥원

PRIVACY REPORT

2024 개인정보보호 월간동향분석

| CONTENTS |

2024년 10월호

CJEU, GDPR

슈렘스 사건 등 CJEU의 최근 개인정보보호 관련 판례 분석

[목 차]

1. 개괄

▌'24년 10월 4일, EU 사법재판소(Court of Justice of the European Union, 이하 CJEU)는 EU 일반 개인정보보호법(이하 GDPR) 일부 조항의 해석과 관련해 주목할 만한 결정을 잇달아 내림

- CJEU는 그간 네덜란드를 중심으로 논란이 되었던, GDPR 제6조제1항제f호 '정당한

이익'에 상업적 이익이 포함될 수 있는지 여부에 대한 중요한 해석을 제시

- 그밖에도 건강 관련 개인정보의 광범위성, 맞춤형 광고 목적으로 온라인 플랫폼에서 처리할 수 있는 개인정보 범위, 동법 제82조 법문 해석 등에 관해서도 기존의 불확실성을 일부 해소
- 아래에서는 CJEU가 같은 날 공개한 결정 5건을 각각 사실관계, 쟁점, 결정 순으로 차례로 살펴보기로 함

2. C-446/21 : 슈렘스(Schrems) 사건(맞춤형 광고 관련)

(1) 개요

▌CJEU는 온라인 소셜 네트워크 플랫폼이 플랫폼 외부에서 수집한 개인정보를 정보주체에 대한 맞춤형 광고 목적으로 활용할 수 없다고 판시

- 정보주체가 공개 토론에서 자신의 성적 지향과 관련해 진술했다는 사실만으로 온라인 소셜 네트워크 플랫폼이 해당 정보주체의 성적 지향과 관련된 기타 개인정보를 수집, 분석하여 맞춤형 광고를 제공할 수는 없음

(2) 사실관계 및 쟁점사항

▌프라이버시 관련 비영리단체 noyb(none of your business)의 대표 막시밀리안 슈렘스(Maximillian Schrems)는 Meta Platforms Ireland(이하 Meta)를 상대로 개인정보의 부적절한 처리와 관련해 오스트리아 관할 법원에 소송 제기

- 슈렘스는 Facebook 운영 주체인 Meta가 본인의 개인정보, 특히 공개 패널 토론에서 언급한 성적 지향에 대한 정보를 불법적으로 처리했다고 주장
- Meta는 쿠키, 소셜 플러그인 등을 활용하여 Facebook 이용자의 소셜 네트워크 안팎에서의 활동에 관한 개인정보, 특히 온라인 플랫폼 방문 및 타사 웹사이트 등과 관련된 개인정보를 수집해 옴

▌이와 관련, 오스트리아 대법원은 CJEU에 GDPR의 해석에 대한 선결적 판단을 구하기 위해 사건을 회부했으며, 주요 쟁점은 다음과 같음

- GDPR 제5조제1항제c호의 '개인정보 최소화 원칙'이 소셜 네트워크 플랫폼의 모든 개인정보를 시기나 정보 유형에 관계 없이 맞춤형 광고에 활용하는 것을 금지하는지 여부
- GDPR 제5조제1항제b호 및 제9조제2항제e호에 근거하여 온라인 소셜 네트워크 플랫폼이 개인이 공개적으로 언급한 성적 지향에 관한 개인정보를 맞춤형 광고 목적으로 처리할 수 있는지 여부

(3) CJEU의 판단

▌CJEU는 정보주체의 일회성 공개 발언이 모든 관련 개인정보 처리에 대한 포괄적 동의로 해석될 수 없으며, 각각의 개인정보 처리에 대해 별도의 법적 근거가 필요하다고 판시

- (개인정보 최소화 원칙) CJEU는 소셜 네트워크 플랫폼 운영자를 비롯한 컨트롤러가 정보 유형을 막론하고 모든 개인정보를 맞춤형 광고 목적으로 집계, 분석 및 처리하는 것은 개인정보 최소화 원칙에 반한다고 판단
- (민감정보의 활용) CJEU는 개인이 공개적으로 밝힌 성적 지향에 관한 정보는 GDPR 제9조제1항(특별 범주의 개인정보 처리)에 따라 원칙적으로 금지되나, 동조 제2항에 따라 예외적으로 처리될 수 있다고 해석
  - CJEU는 슈렘스의 공개 발언이 GDPR 제9조제2항제a호에 규정된 바와 같이 슈렘스가 Meta의 개인정보 처리에 대해 '명시적 동의'를 제공한 것으로 볼 수 없다고 판단
  - 다만, CJEU는 해당 공개 발언이 GDPR 제9조제2항제e호에 규정된 대로 개인정보가 명시적으로 공개된 것이라면 개인정보의 예외적 처리가 가능한지 여부를 살펴볼 필요가 있다고 언급
  - 이와 관련, CJEU는 그러한 공개 발언 사실만으로 소셜 네트워크 플랫폼이 플랫폼 외부에서 제3자 웹사이트나 앱을 통해 수집한 성적 지향 관련 정보를 수집, 분석하여 맞춤형 광고를 제공하는 데에 활용할 수 있다고 보기는 어렵다고 결론

3. C-21/23 : 온라인 의약품 판매 사건

(1) 개요

▌CJEU는 부적절한 개인정보 처리가 불공정한 상행위에 해당하는 사안에서, 경쟁사가 GDPR 위반을 근거로 불공정 상행위임을 주장하며 법원에 소송을 제기하는 것이 금지되지 않는다고 판시

- CJEU는 GDPR 조항 위반으로 인해 불법을 저지르는 사업자의 경쟁사가 EU회원국의 국내법상 불공정 상행위를 근거로 소송을 제기할 수 있는 권한을 그대로 가진다고 해석
- 이와 관련, CJEU는 건강 관련 개인정보를 보다 광범위하게 해석하여, 정보의 조합 등 추론을 통해 개인의 건강 관련 상태를 도출할 수 있다면 GDPR에서의 건강 관련 개인정보로 볼 수 있다고 해석

(2) 사실관계 및 쟁점사항

▌약국을 운영하는 약사 A는 약국 전용 일반의약품(처방전이 필요하지 않지만 약국에서만 판매하는 의약품) 및 다양한 의약품을 온라인을 통해 판매

- 약사A는 고객으로 하여금 의약품 주문 과정에서 이름, 배송 주소, 의약품 세분화 정보 등을 제공하도록 함
- 이에 약사B는 약사A의 개인정보 수집 행위가 정보주체의 건강 개인정보를 처리하는 것이라 주장, 이를 법률을 위반한 상행위로서 불공정 경쟁 금지법을 근거로 관할 법원에 해당 판매 행위의 중지를 구하는 소송을 제기

▌독일 연방법원은 심리 과정에서, GDPR에 대한 법적 해석이 필요하다고 판단, CJEU에 GDPR 해석을 위한 선결적 판단을 요청

- (약사B의 청구권 관련) 개인정보보호 침해를 직접적으로 당한 정보주체가 아닌 제3자(이 사건에서는 약사B)가 GDPR 제8장(제77조~제84조)의 규정에도 불구하고 GDPR 위반이 불공정 상행위에 해당함을 주장하면서 불공정 경쟁 금지법을 근거로 법원에 소송을 제기할 수 있는지 여부
- (건강 개인정보의 범위) 처방전이 필요한 전문의약품이 아닌 경우에도 고객이 온라인 구매 과정에서 제공하는 고객 정보(이름, 배송 주소, 의약품 세분화 정보)가 GDPR 제9조제1항에서의 건강 관련 개인정보에 해당하는지 여부

(3) CJEU의 판단

▌CJEU는 GDPR 규정이 EU 회원국의 국내법에 따른 소송권한을 배제하지 않으며, 온라인 주문 과정에서 입력하는 정보 또한 건강 개인정보에 포함된다고 판시

- CJEU는 정보주체가 아닌 제3자 또한 상대방의 GDPR 위반으로 인해 피해를 입었다면 GDPR 위반을 주장하며 국내법에 근거하여 법원에 소송을 제기할 수 있다고 해석
  - GDPR 제8장은 개인정보 관련 침해를 당한 정보주체가 관할 감독기관이나 법원에 민원 또는 소송을 제기할 수 있는 권리를 규정
  - 그러나, GDPR 제82조제1항의 문언에서 '동법 위반으로 인해 물질적 또는 비물질적 손해를 입은 모든 사람'의 손해 배상 권리를 명시하고 있어, 동조가 정보주체가 아닌 제3자의 GDPR 위반 관련 소송권을 배제하는 것이라고 해석하는 것은 부적절
  - 경쟁사가 GDPR 위반에 따른 소송을 제기할 수 있다면, 해당 민사소송을 통해 GDPR의 실질적 효과를 높이고 정보주체의 개인정보보호 효과도 누릴 수 있으므로, 이와 같은 해석은 정보주체의 개인정보에 대한 일관되고 높은 수준의 보호를 보장하려는 GDPR의 목적에도 부합
- 또한 CJEU는 건강 관련 개인정보는 다른 특수 범주의 개인정보와 마찬가지로 광범위하게 해석하는 것이 타당하다고 봄
  - 이 사건에서 고객에게 요구한 개인정보는 이름, 배송 정보 등에 불과하나 해당 정보와 고객의 기타

개인정보 등을 조합하면 추론을 통해 얼마든지 개인의 건강상태에 대한 정보가 드러날 수 있기 때문

- 처방전이 필요한 전문의약품과 관련해 제공하는 고객의 정보에 한정하여 건강 관련 개인정보로 분류해야 한다는 반론에 대해서는, 이와 같은 주장이 정보주체에 대한 높은 수준의 보호를 추구하는 GDPR의 취지에 부합하지 않는다고 반박
- 따라서 CJEU는 독일 연방 법원이 약사A의 건강 개인정보 처리가 GDPR 제9조제2항에 따른 예외사유 중 하나에 해당하여 적법하게 처리가 허용되는 것인지 여부를 살펴보아야 한다고 결론

※ 고객의 건강 개인정보 제공에 관한 명시적 동의 여부, 또는 동조 동항 제h호에 근거하여 건강 관리 목적상 필요하거나 법률 또는 계약에 따라 처리가 허용되는지 여부 등

4. C-621/22 : 회원 개인정보 판매 사건

(1) 개요

▌CJEU는 컨트롤러의 상업적 이익 또한 GDPR 제6조제1항제f호의 '정당한 이익'에 포함될 수 있다고 해석

- CJEU는 이 사건 판단에서 GDPR 제6조제1항제f호의 '정당한 이익'을 광범위하게 해석할 수 있다고 보면서, 상업적 이익 또한 정당한 이익에서 반드시 배제되지는 않는다고 판시
- 다만 어떠한 이익이든 상기 '정당한 이익'에 포함되기 위해서는 CJEU가 제안하는 3단계 요건을 모두 충족해야 한다고 강조

(2) 사실관계 및 쟁점사항

▌'19년 12월, 네덜란드 개인정보 감독기관은 네덜란드 테니스 협회(De Koninklijke Nederlandse Lawn Tennisbond(이하 KNLTB))가 스포츠 제품 판매사 및 도박 및 카지노 게임 제공사에 회원의 개인정보를 판매한 점을 들어 52만 5,000유로의 벌금을 부과

- 이때 제공된 개인정보에는 각각 30만명 및 5만명의 회원 이름, 성별 및 주소가 포함되어 있었으나, KNLTB는 개인정보 공유 행위 또한 상업적 이익을 위한 행위로서 GDPR 제6조제1항제f호의 '정당한 이익'에 해당한다고 주장
- 네덜란드 개인정보 감독기관은 개인정보 판매행위와 같은 상업적 이익은 '정당한 이익'에 포함될 수 없다고 반박
- KNLTB는 동 감독기관의 결정에 불복하여 관할 법원에 소송을 제기

▌네덜란드 관할 법원은 그간 네덜란드 내에서 논란이 되었던 GDPR 제6조제1항제f호의 '정당한 이익'의 해석에 대해 CJEU에 선결적 판단을 요청

- 네덜란드 법원은 CJEU에 '정당한 이익'이 법률에 명시된 이익만을 포함하는지, 또는 법률과 저촉되지 않는 모든 이익이 모두 정당한 이익에 포함될 수 있는지, 특히, 컨트롤러의 상업적 이익이 '정당한 이익'으로 간주될 수 있는지 여부를 질문

(3) CJEU의 판단

▌CJEU는 네덜란드 법원의 질문에 대해 직접적인 답변은 피하면서도, 특정 이익이 '정당한 이익'으로 분류될 수 있는지 여부를 가늠하는 3단계 요건을 제시

- (정당성) CJEU는 컨트롤러가 주장하는 이익이 정당하다면 반드시 법률에 명시될 필요는 없다고 정당한 이익을 광범위하게 해석하면서, 다만 컨트롤러가 GDPR 제13조1항제d호에 따라 개인정보를 수집할 때 GDPR 제6조1항제f호의 정당한 이익을 주장하기 위해서는, 법문에 따라 해당 정당한 이익에 대해 정보주체에게 알려야 할 의무가 있다고 판단
  - 따라서, 이 사건 KNLTB가 광고 또는 마케팅 목적으로 제3자에게 회원 개인정보를 대가를 받고 판매하는 '상업적 이익'은 법률에 위배되지 않는 한 정당한 이익을 구성할 수 있음
- (필요성) CJEU는 컨트롤러가 추구하는 정당한 이익이 정보주체의 기본적 권리와 자유에 대한 침해가 덜한 여타 방식으로는 합리적 및 효과적으로 달성될 수 없어야 한다고 강조
  - 이 사건에서 CJEU는 KNLTB가 회원의 개인정보를 제3자에게 제공하고자 할 경우 정당한 이익을 주장하지 않더라도 해당 제공 사실을 회원에게 알리고 광고 또는 마케팅 목적으로 해당 제3자에 개인정보를 제공하는 것에 동의하는지 여부를 사전에 묻는 방식으로 개인정보 처리가 가능했을 것이라고 지적
- (균형성) CJEU는 또한 정보주체의 권리 및 이익이 컨트롤러 등 제3자의 정당한 이익보다 중요하지 않아야 한다고 언급
  - CJEU는 각 회원국 법원이 균형성 단계 검토 과정에서, 정보주체의 합리적 기대, 개인정보 처리의 규모, 정보주체에게 미치는 영향 등을 고려해야 한다고 밝히며,
  - 이 사건의 경우 회원이 자신의 개인정보가 제3자에게 판매되는 것을 합리적으로 기대하지 않는 상황에서 개인정보가 제3자에게 제공된 경우라면, 정보주체의 이익이 컨트롤러의 이익보다 중요할 수 있다고 결론

5. C-200/23 : 정관 문서 개인정보 공개 사건

(1) 개요

▌CJEU는 GDPR 제82조제1항에 규정된 '비물질적 손해'에 대해 정보주체에게 추가적인 유형적 피해

를 입증할 것을 요하지 않는다고 판시

- CJEU는 동조의 '비물질적 손해'는 정보주체가 실제 피해를 입었다는 사실을 입증하는 것으로 족하며, 이를 넘어 정보주체에게 추가적으로 유형적인 피해 결과를 입증할 것을 요구할 수는 없다고 언급

(2) 사실관계 및 쟁점사항

▌이 사건 정보주체는 불가리아 소재 회사의 주주로, 회사의 정관 문서가 공공 상업 등록부를 관리하는 관할 당국(Agentsia po vpisvaniyata, 아겐치야 포 브피스바니야타)에 전송된 바 있음

- 해당 정관 문서에는 해당 주주의 성, 이름, 식별 번호, 신분증 번호, 해당 신분증의 발급 날짜 및 장소, 주소 및 서명이 포함되어 있었으며, 해당 정관 문서는 제출된 즉시 대중에게 공개됨
- 정보주체는 정관 문서에 회사와 무관한 자신의 기타 개인정보가 포함된 것을 확인하고 등록 기관(Agentsia po vpisvaniyata)에 삭제를 요청
- 등록 기관(Agentsia po vpisvaniyata)은 상업 등록부에 회사와 관련된 특정 정보를 공개해야 하는 법적 요건이 있고, 정보주체가 추가적인 개인정보의 공개를 원하지 않았을 경우 (미리 개인정보가 삭제된) 편집된 정관 문서를 제출했어야 한다고 주장하며 삭제 요청을 묵시적으로 거부

▌정보주체는 행정법원에 해당 거부 행위의 취소를 구하는 소송을 제기

- 정보주체는 등록 기관(Agentsia po vpisvaniyata)의 묵시적 거부에 대해 행정 법원에 소송를 제기하였으며, 행정법원은 등록 기관의 묵시적 거부 행위에 대해 취소를 명령
- 등록 기관은 우편으로 개인정보를 일부 가린 사본을 첨부하면서, 법률에서 공개를 요구하는 사항을 제외하고 해당 정보주체의 개인정보를 모두 숨김처리했다고 주장
- 이에 정보주체는 다시 행정법원에 소송을 제기하며 등록 기관(Agentsia po vpisvaniyata)의 우편 발송행위의 취소 명령을 구함과 동시에. GDPR에서 부여한 권리를 침해당했음을 이유로 비물질적인 손해를 배상하도록 해달라고 주장
- 행정법원은 정보주체의 주장대로 등록 기관의 우편 발송행위의 취소를 명령하고, 해당 기관이 GDPR 제82조에 따라 정보주체에게 비물질적 손해에 대해 배상하라고 결정
- 등록 기관(Agentsia po vpisvaniyata)은 행정법원의 판단에 불복하여 최고 행정법원에 상고

▌불가리아 최고 행정법원은 심리 과정에서 GDPR 여러 조항의 해석에 대한 명확성이 필요하다고 판단, 아래에 거론된 조항에 대한 선결적 판단을 구하기 위해 사건을 CJEU에 회부

- ▲ 등록 기관이 GDPR 제4조제7항 및 제9항에 따라 개인정보의 수령인이자 컨트롤러에 해당하는지 여부 ▲해당 기관의 GDPR 제17조에 따른 개인정보 삭제 의무 여부 ▲서명이 GDPR 제4조제1항에

따른 개인정보에 해당하는지 여부 ▲부적법하게 처리된 개인정보의 공개로 인한 피해가 어디까지 입증되어야 하는지에 대한 제82조제1항 해석 ▲감독기관의 의견에 따라 행동하던 와중에 피해를 입힌 경우 GDPR 제82조제3항에 따라 책임이 면제될 수 있는지 여부

(3) CJEU의 판단

▌CJEU는 불가리아 최고 행정 법원의 GDPR 해석 요청에 대해 다음과 같이 판시

- (등록 기관의 컨트롤러 여부 등) 등록 기관(Agentsia po vpisvaniyata)은 정관 문서에 포함된 개인정보의 수령인으로서, 해당 문서에 법률에서 요구하지 않는 개인정보가 포함되어 있더라도 해당 개인정보를 대중에게 공개하는 상황에서는 여전히 동법 제4조제7항에 따른 컨트롤러로 간주됨
- (삭제 의무) 상업 등록부를 관리하는 컨트롤러는 정보주체의 개인정보 과다 제공 등을 들어 등록부에 게시된 개인정보 삭제 요청을 단호하게 거부할 수 없음
  - 정보주체는 자신의 이익에 우선하는 정당한 이익이 없는 한 개인정보 처리에 반대할 권리와 삭제 권리를 가짐
- (서명의 개인정보성) 자연인의 친필 서명은 일반적으로 개인을 식별하는 데 사용되고 문서의 정확성과 진위 여부에 대한 증거로서 효력을 가지므로 동법 제4조제1항에 따른 '개인정보'로 간주될 수 있음
- (비물질적 피해의 입증 범위) EU회원국 상업 등록부상의 개인정보가 온라인으로 공개됨으로써 정보주체가 일정 기간 동안 자신의 정보에 대한 통제권을 상실한 경우 동법 제82조제1항에 따른 '비물질적 손해'를 유발하기에 충분할 수 있다고 해석하는 것이 타당
  - 이 경우 정보주체 자신이 실제로 그러한 손해를 입었다는 것을 입증해야 하며, 다만 '비물질적 손해'라는 개념이 추가적인 유형적 손해를 입증할 것을 요하는 것은 아님
- (책임 면제 여부) 회원국 개인정보 감독기관이 GDPR 제58조3항제b호에 근거하여 의견을 발행하고 컨트롤러가 해당 의견에 따라 행동하더라도, 이러한 사유만으로 GDPR 제82조제3항에 규정된 책임 면제에 해당될 수 없음
  - GDPR 제58조3항제b호에서 '의견' 및 '자문' 권한이라는 용어를 사용한 것은 이 조항에 따라 발행된 의견이 EU법에 따라 법적 구속력이 없음을 나타냄
  - 따라서 컨트롤러에 발행된 감독기관의 의견은 법적 구속력이 없고 정보주체가 입은 손해가 컨트롤러로부터 기인하지 않음을 입증할 수 없으므로 컨트롤러가 책임을 면하기에 충분하지 않음

6. C-507/23 : 언론인 사건

(1) 개요

▌CJEU는 사과의 표현만으로도 GDPR 제82조제1항에 따른 '비물질적 손해'에 대한 충분한 배상이 될 수 있다고 판단

- 피해 발생 전으로 상황을 되돌릴 수 없고 사과가 정보주체가 입은 피해를 완전히 보상할 수 있는 경우, 사과가 비물질적 손해에 대한 적절한 배상 수단으로 작용할 수 있음

(2) 사실관계 및 쟁점사항

▌라트비아 소비자 권리 보호 센터는 자동차 전문 기자였던 정보주체의 동의 없이 해당 정보주체를 모방한 캐릭터를 활용하여 중고차 위험 관련 비디오 캠페인을 진행

- 정보주체는 동 센터에 자신을 모방한 캐릭터가 등장하는 비디오 캠페인을 삭제하고 명예훼손에 대한 손해배상을 청구하기 위해 라트비아 행정법원에 소송을 제기
- 소송에서 동 센터의 행위는 불법으로 판단되었지만 명예훼손에 따른 손해배상의 경우 비디오 캠페인의 의도가 신청인의 명예훼손이 아니라 공익 목적의 업무 수행에 있다고 보아 기각됨

▌정보주체가 이에 불복하여 상급심이 진행되던 중, 라트비아 대법원이 GDPR 제82조제1항과 관련한 일부 해석을 명확하게 하기 위해 사건을 CJEU에 회부

- GDPR 제82조제1항이 불법적인 개인정보 처리 그 자체로서 개인정보보호 권리에 대한 부당한 간섭을 구성하고 해당 개인에게 피해를 입힐 가능성이 있다는 의미로 해석될 수 있는지 여부
- GDPR 제82조제1항이 비물질적 손해에 대한 유일한 구제 수단으로써 사과를 허용하는지 여부
- GDPR 제82조제1항에 따른 손해배상액 판단 시 컨트롤러의 태도 및 동기가 고려 대상인지 여부

(3) CJEU의 판단

▌CJEU는 라트비아 법원의 해석 요청에 대해 아래와 같이 판시

- GDPR 위반 자체로는 동법 제82조제1항의 배상을 요하는 '손해'를 구성하기에 충분하지 않으며, 이렇게 해석하는 것이 유럽연합 기본권 헌장 제8조제1항(개인정보를 보호받을 권리)의 취지에도 부합
- 정보주체의 상태를 피해 발생 전으로 되돌리는 것이 불가능한 경우, 사과는 비물질적 손해에 대한 적절한 배상으로 간주될 수 있으며, 이때 사과는 정보주체가 입은 손해를 충분히 보상하는 것에 해당됨
- 정보주체에게 지급할 배상액을 법원이 결정할 때 컨트롤러의 태도와 동기는 액수의 가중 또는 감경 사유로 고려될 수 없는데, 이는 GDPR 제82조가 처벌적 기능이 아닌 배상적 기능을 수행하기 때문

출처 |

1. A&O Shearman, CJEU: Commercial interests of controller can serve as a legitimate interest, 2024.10.09.
2. Court of Justice of the European Union, PRESS RELEASE No 159/24 (Judgment of the Court in Case C-21/23 | Lindenapotheke), 2024.10.04.
3. Court of Justice of the European Union, PRESS RELEASE No 166/24 (Judgment of the Court in Case C-446/21 | Schrems (Communication of data to the general public)), 2024.10.04.
4. DataGuidance, EU: CJEU publishes judgment on compensation for non-pecuniary damages, 2024.10.04.
5. Dentons, CJEU Judgement: KNLTB-case, 2024.10.16.
6. DLA Piper, EU: CJEU Confirms that Legitimate Interests can cover purely commercial interests, 2024.10.07.
7. DLA Piper, EU: CJEU Insight, 2024.10.15.
8. DLA Piper, EU: ECJ rules that competitors are entitled to bring an injunction claim based on an infringement of the GDPR, 2024.10.07.
9. Jan Sandtro, C-200/23 Agentsia po vpisvaniyata, 2024.10.
10. Lexology, GDPR-infringements as unfair commercial practice - did the CJEU just give superpower to competitors?, 2024.10.24.
11. Matheson, CJEU Publishes a Flurry of GDPR-related Decisions, 2024.10.23.
12. Portolano Cavallo, CJEU ruling: Competitors granted legal standing to challenge GDPR violations as unfair competition, 2024.10.24.

AI 안전성

호주 정부, 고위험 AI 안전장치 제안 협의 및 자발적 AI 안전 표준 발표

[목 차]

1. 배경

▌호주는 최근까지 AI에 특화된 포괄적인 규제 프레임워크를 운영하지 않고 있었으며, 기존의 일반 규제 체계 내에서 AI 관련 이슈를 다루어 왔음

- 그러나 호주 정부는 급속도로 발전하는 AI 기술과 그에 따른 사회적 변화에 대응하기 위해 현행 규제 체계의 개선 필요성 인식
- 특히 AI가 야기할 수 있는 고유한 위험에 대응하기 위해 예방적이고 위험기반의 안전장치 도입을 고려

▌'24년 9월 5일, 호주 연방 정부는 AI 개발 및 배포에 대한 안전 가이드라인에 관한 협의를 개시하고 자발적 AI 안전 표준 또한 발표

- 호주 산업과학자원부(DIRS, Department of Industry, Science and Resources)는 기술 혁신을 저해하지 않으면서도 균형 잡힌 AI 규제 체계를 마련하고자 두 가지 문서를 발표
  - 고위험 AI 환경에서의 필수 안전장치 도입을 포함한 제안서(Proposal paper for introducing mandatory guardrails for AI in high-right settings, 이하 "제안서")
  - 자발적 AI 안전 표준(Voluntary AI Safety Standards)
- 해당 제안서는 고위험 AI 환경에 적용되는 필수 안전장치와 '고위험 AI'의 정의 방식,

안전장치 의무화를 위한 규제 옵션에 대해 제안하며, 호주 정부는 '24년 10월 4일까지 이에 대한 공개 의견 수렴을 진행함

- 자발적 AI 안전 표준은 모든 호주 조직이 AI를 안전하고 책임감 있게 사용 및 혁신할 수 있도록 지원하는 실질적인 지침으로, 필수 안전장치의 시행에 앞서 기업들에게 규제 확실성을 제공하고자 마련[1)]

▌호주 정부는 AI의 안전한 사용을 보장하고, 기업들에게 규제적 확실성을 제공하며, AI 기술의 혜택을 극대화함과 동시에 AI 공급망 전반과 AI 수명 주기 전체에 적용 가능한 안전장치 도입을 고려하고자 함

- 이러한 조치를 통해 정부는 AI 기술 발전에 따른 위험을 적절히 관리하면서도 혁신을 촉진하는 균형 잡힌 접근법을 추구하고 있음
- 이하에서는 산업과학자원부(DIRS)가 공개한 동 제안서와 자발적 AI 안전 표준의 주요 내용 소개

2. 고위험 AI 설정에 대한 필수 안전장치 제안서

(1) 위험기반 접근법 및 고위험 AI 정의

▌동 제안서는 필수 안전장치(mandatory guardrails)의 적용 대상으로 '고위험 AI(high-risk AI)'에 초점을 둠

- 앞서 호주 정부는 초기 협의 당시 전문가 자문단의 조언을 바탕으로, AI가 다른 유형의 소프트웨어 프로그램과 구별되는 특성을 보유하고 있어 특정 규제 대응이 필요하다고 판단한 바 있음
  - 특히 AI로 인해 증폭되는 기존 및 신규 위험 요소(예: 편향과 차별, 허위정보, 개인정보 침해 등)에 대해 사전 예방적인 조치에 중점을 둔 위험기반 접근법이 필요함을 강조

표 1 다른 국가들에서 식별된 고위험 AI 사용 사례[2)]

분야	세부 설명
생체 인식	• 개인을 식별하거나 분류하고, 행동 또는 정신 상태를 평가하거나 감정에 영향을 미치기 위해 사용되는 AI 시스템

1) Minister for Industry and Science, "The Albanese Government acts to make AI safer", 2024.9.5. (URL: https://www.minister.industry.gov.au/ministers/husic/media-releases/albanese-government-acts-make-ai-safer) 참고

주요기반시설	• 주요 디지털 인프라, 교통, 수자원, 가스, 난방 및 전기 공급의 관리 및 운영에서 안전 요소로 사용되는 AI 시스템
교육/훈련	• 교육 프로그램 입학 결정, 학습 성과 평가, 학생 행동 모니터링에 사용되는 AI 시스템
고용	• 채용, 추천, 채용, 급여, 승진, 교육, 견습, 이동 또는 해고 등 고용 관련 결정에 사용되는 AI 시스템
필수 공공 서비스 및 제품 접근	• 의료, 사회 보장 혜택 및 신흥 서비스 등 개인에게 제공되는 서비스 접근 유형과 범위를 결정하기 위해 사용되는 AI 시스템
필수 민간 서비스 접근	• 신용, 보험 등 필수 민간 서비스에 대한 접근에 영향을 미치고 상당한 위험을 수반하는 방식으로 결정하기 위해 사용되는 AI 시스템
개인 및 공공 건강 및 안전에 영향을 미치는 제품 및 서비스	• 제품의 안전 요소로 사용되거나, 개인 및 공공 건강과 안전에 영향을 미치는 제품으로 의도된 AI. 여기에는 AI 기반 의료기기, 식품 제품 및 기타 상품과 서비스가 포함됨
법 집행	• 개인 프로파일링, 재범 위험 평가, 폴리그래프 스타일 기술 또는 증거 평가와 같은 법 집행 분야에서 사용되는 AI 시스템
사법 및 민주적 절차 관리	• 법원 또는 행정 심판에서 개인에 대한 결정을 내리거나 사실, 증거 및 제출 절차를 평가하기 위해 사용되는 시스템 • 민주적 절차와 관련하여, 개인의 투표 행동이나 선거 또는 민주적 절차의 결과에 영향을 미칠 수 있는 모든 시스템을 포함할 수 있음

출처: 제안서 내용을 기반으로 넥스텔리전스(주) 재구성

▌'고위험 AI'를 정의함에 있어, 동 제안서는 의무적 안전장치가 적용되는 두 가지 범주를 제시

- (범주 1) AI 시스템*이나 범용 AI 모델(GPAI 모델, general-purpose AI model)**의 제안된 사용이 **알려져 있거나 예측 가능한 경우(known or forseeable)**와 관련된 '고위험'

  * AI 시스템(AI system)이란, 하나 이상의 AI 모델을 포함한 여러 구성 요소의 집합체로, 인간에게 특정한 방식으로 유용하도록 설계된 시스템으로 정의. AI 모델이 AI 애플리케이션의 '엔진' 역할을 하는 수학적 본질이라면, AI 시스템은 이를 포함하여 실제로 사용 가능한 형태로 구현된 전체 시스템을 의미(예: ChatGPT 앱은 AI 시스템이며, 이 시스템의 핵심 엔진인 GPT-4는 AI 모델에 해당)

  ** 다양한 목적으로 사용되거나 사용을 위해 적응될 수 있는 AI 모델로, 직접 사용뿐만 아니라 다른 시스템에 통합될 수 있는 능력을 갖춘 모델

  - 이때 위험은 AI 시스템이 사용될 맥락이나 AI 시스템 또는 GPAI 모델의 예측 가능한 응용 프로그램을 참조하여 결정됨

- (범주 2) 모든 가능한 응용 프로그램과 위험을 예측할 수 없는 **'고급 고성능 GPAI 모델(advanced, highly-capable GPAI models)'**과 관련된 '고위험'

  - 이러한 모델은 다양한 목적으로 사용되거나 오용될 수 있는 잠재력에 위험 존재

2) 이는 캐나다와 유럽연합(EU)의 사례를 참고하고 있음. 제안서 11~12, 16, 26~27 pp. 참고

- 첫 번째 범주와 관련하여 동 제안서는 다음과 같은 원칙 기반의 정의를 제시:
  - AI 시스템 사용으로 인한 고위험으로 지정할 때 다음 사항을 고려해야 함
    (a) 호주 인권법에서 인정하는 개인의 권리에 대한 부당한 악영향의 위험
    (b) 개인의 신체적 또는 정신적 건강이나 안전에 대한 악영향의 위험
    (c) 개인에 대한 부정적인 법적 영향, 명예훼손 또는 유사하게 중대한 영향의 위험
    (d) 개인 집단이나 문화 집단의 집단적 권리에 대한 악영향의 위험
    (e) 호주의 경제, 사회, 환경 및 법치주의에 대한 광범위한 악영향의 위험
    (f) 위의 (a)부터 (e)까지 열거된 악영향의 심각성과 범위
- 두 번째 범주에 대해, 제안서는 GPAI 모델에 대한 별도의 위험 기준이나 임계값을 제안하지 않으나, 대신 모든 GPAI 모델의 개발과 배포에 의무적 안전장치를 적용할 것을 제안
  - 이는 GPAI 모델이 원래 설계되지 않은 맥락에서 적용될 수 있기 때문(즉, 예측 불가능한 위험)
  - 제안서는 "현재 대부분의 고성능 GPAI 모델이 국내에서 개발되지 않고 있으므로, 산업계와 정부 모두의 규제 준수 부담을 줄이고 혁신을 촉진하는 규제 환경을 조성하기 위해 다른 국제 관할권과의 조화가 중요하다"고 인정하고 있음

(2) 필수 안전장치

▌동 제안서는 고위험 환경에서 사용되는 AI 시스템과 GPAI에 대한 10가지 의무적 안전장치 제시

- 각 안전장치는 사전예방적 성격을 보이며, 전반적으로 테스트, 투명성, 책임성에 중점을 둠
  - 이러한 안전장치는 정적인 것이 아니며, 기술 발전에 맞추어 진화할 수 있게 설계
  - 피해가 발생했을 때 시정 및 집행 조치를 가능하게 하는 법률 및 규제 수단과 함께 작동해야 함
  - 또한, 이러한 안전장치는 다른 유사한 관할권에서 개발 및 채택한 안전장치와 상호 운용이 가능하도록 설계되었음
  - 안전장치는 AI 시스템의 개발자(developer)와 배포자(deployer)가 구현해야 하며, 책임은 다양한 상황적 요인에 의거하여 배분될 예정

▌제안된 필수 안전장치는 대체로 '자발적 AI 안전 표준'에 포함된 것들과 일치하나, 제안서와 표준은 10번째 안전장치에서 차별성을 보임

- ① 거버넌스, 내부 역량 및 규정 준수 전략을 포괄하는 책임 프로세스의 수립, 구현 및 공개

- 고위험 AI 시스템을 개발하거나 배포하는 조직은 안전장치 준수를 보장하기 위해 거버넌스 정책과 명확한 역할을 포함한 책임 절차를 마련하고, 이러한 절차는 대중의 AI 제품 및 서비스에 대한 신뢰 향상을 위해 공개되고 접근 가능해야 함

• ② 위험 관리 프로세스 구축 및 실행

- 조직은 고위험 AI 시스템에서 발생하는 위험을 관리하기 위한 위험 관리 절차를 수립, 실행, 유지해야 하며, 개발자와 배포자는 시스템 사용 전 개인, 공동체, 사회에 미칠 잠재적 영향을 고려하고, 위험 제거가 불가능한 경우 이를 억제하거나 완화할 수 있는 전략을 마련해야 함

• ③ AI 시스템 보호 및 데이터 거버넌스 조치 구현

- 조직은 적절한 데이터 거버넌스, 개인정보 보호 및 사이버 보안 조치를 갖추어야 하며, 모델의 학습, 미세 조정 또는 테스트에 사용되는 데이터가 목적에 부합하고 대표성을 가지며 불법적이거나 유해한 자료를 포함하지 않도록 해야 함

- 또한, 데이터는 합법적으로 확보된 것이어야 하며 출처를 공개하고, 무단 접근 및 악용으로부터 보호될 수 있도록 저장 및 관리되어야 함

• ④ AI 모델·시스템의 성능 평가 및 지속적인 시스템 모니터링

- 조직은 고위험 AI 시스템을 시장에 출시하기 전 AI 모델의 성능을 테스트하고 평가해야 하며, 시스템이 예상대로 작동하도록 지속적으로 모니터링해야 함

- 또한, AI 모델은 용도와 관련 위험에 따라 달라지는 구체적이고 객관적이며 측정 가능한 성능 지표를 충족해야 함

• ⑤ AI 시스템의 수명 주기 전반에 걸친 의미있는 인간 통제 보장

- 조직은 고위험 AI 시스템을 사람이 이해하고 감독하며 필요 시 개입할 수 있도록 AI 공급망과 수명 주기 전반에서 관리 체계를 마련해야 함

- 감독 담당자는 AI 모델의 핵심 능력과 한계를 이해하고 출력을 해석할 수 있는 충분한 자격을 갖추어야 함

• ⑥ 최종 사용자(end-user)에게 AI를 활용한 결정, AI와의 상호작용 방식, AI 생성 콘텐츠에 대한 정보 투명하게 공개

- 조직은 최종 사용자에게 AI 사용 방식과 그 영향에 대해 명확하고 접근 가능한 방식으로 알려야 하며, 이를 위해 다음 세 가지가 요구됨

  (1) AI가 사용자와 관련된 의사결정을 내리거나 영향을 미칠 때 이를 알릴 것

  (2) 사용자가 AI 시스템과 직접 상호작용할 때 이를 알릴 것

(3) 합성 텍스트, 이미지, 오디오 등 AI 생성 출력물이 인공적으로 생성되었음을 식별할 수 있도록 최선을 다할 것

- ⑦ AI 시스템의 영향을 받는 사람들이 AI 사용이나 결과에 대해 이의를 제기할 수 있는 절차 수립
  - 조직은 고위험 AI 시스템으로 인해 부정적 영향을 받은 사람들이 AI 결정에 이의를 제기하거나 불만을 제기할 수 있는 절차를 마련해야 함
- ⑧ 데이터, 모델, 시스템에 대해 AI 공급망 전반의 다른 조직과 투명하게 공유하여 위험을 효과적으로 해결할 수 있도록 지원
  - 조직은 고위험 AI 시스템의 개발 및 운영에 참여하는 다른 관계자들과 정보를 공유하여 AI 공급망 전반의 투명성을 높이고 법적 의무 준수와 위험 식별 및 완화를 돕도록 해야 함
  - 개발자는 배포자에게 AI 시스템의 사용 방법과 출력 해석에 필요한 정보를 제공해야 하며, 배포자는 부정적 사건이나 주요 모델 오류를 개발자에게 보고하여 개선이 이루어질 수 있도록 함
- ⑨ 제3자가 안전장치 준수 여부를 평가할 수 있도록 기록 보관 및 유지
  - 조직은 고위험 AI 시스템의 수명 주기 동안 다양한 기록을 보관·유지하고, 요청 시 관련 당국에 제출할 준비가 되어 있어야 하며,
  - 위험한 능력을 지닐 가능성이 있는 최첨단 GPAI 모델을 훈련하는 경우 해당 훈련 기록을 호주 정부에 공개해야 함
- ⑩ 안전장치 준수를 입증(demonstrate)하고 인증(certify)하기 위해 적합성 평가 수행
  - 조직은 고위험 AI 시스템을 시장에 출시하기 전 및 이후에도 지속적으로 안전 장치 준수를 확인하기 위해 자체적으로 또는 제3자, 정부 기관, 규제 기관을 통해 적합성 평가를 실시해야 함

(3) 안전장치 의무화를 위한 규제 옵션

▌제안서는 AI의 개발 및 사용이 소비자 보호, 개인정보보호, 차별 금지, 경쟁, 프라이버시, 저작권 등 다양한 법률체계의 영향 아래 있는 점에 주목

- 특히 호주의 현행 법률체계 및 규제는 일부 AI 위험 요소에 대해서는 대응 가능하나, 다음과 같은 한계가 있음을 언급
  - 특정 AI 특성으로 인한 위험을 예방하거나 완화하는 데 있어 일부 영역에서는 규제 공백과 산업 간 일관성 부족이 존재함

- 각 규제 체계는 규제 범위와 대상에 한정됨
- 규제가 위험 예방보다는 사후 처벌에 중점을 두고 있음
- 규제 체계마다 적용 기준과 처벌 수준이 상이함

▌이에 동 제안서는 위와 같은 현행 규제상의 한계를 해결하고자, 고위험 AI 환경에서의 위험 관리를 위한 세 가지 규제 옵션을 제안하고 있음

- (옵션 1) 기존 규제 체계에 제안된 안전장치를 통합하는 방안
  - 기존의 법적 규제 체계에 안전장치를 포함하여 해당 체계를 수정하는 방식
- (옵션 2) 새로운 규제의 도입에 맞춰 현행법을 개정하는 방안
  - 새로운 법률을 도입하여 필수 안전장치와 적용 기준을 정의하고, 기존의 법률을 이 같은 새로운 법률에 맞춰 개정하는 방식
- (옵션 3) 범경제적(cross-economy) AI 법 제정
  - AI의 고위험 애플리케이션을 정의하고, 필수 안전장치를 설명하며, 독립적인 AI 규제기관이 감독하는 모니터링 및 집행 체제를 구축하는 AI 관련 법을 도입하는 방식

3. 자발적 AI 안전 표준

▌자발적 AI 안전 표준은 조직들이 지속적으로 수행해야 할 10가지 자율 안전장치로 구성

- ① 거버넌스, 내부 역량 및 규정 준수 전략을 포괄하는 책임 프로세스의 수립, 구현 및 공개
  - AI 배포의 안전하고 책임 있는 관리는 외부 위탁이 불가하며, 조직은 AI 책임자 지정, 전략 수립, 정책 구현, 교육 제공 등을 통해 AI 사용을 위한 적절한 내부 기반을 구축할 필요가 있음
- ② 위험 관리 프로세스 구축 및 실행
  - 위험 식별 및 완화를 위한 위험 관리 프로세스를 수립하고, 지속적으로 각 AI 시스템에 대한 위험 및 영향 평가를 수행해야 함
- ③ AI 시스템 보호 및 데이터 거버넌스 조치 구현
  - 조직은 AI의 활용 사례와 위험 프로필에 맞춰 데이터 거버넌스, 개인정보보호, 사이버 보안 조치를 구현하되, 데이터 품질, 출처, 사이버 취약점 등 AI의 고유한 특성을 반드시 고려해야 함
- ④ AI 모델·시스템의 성능 평가 및 지속적인 시스템 모니터링

- AI 시스템은 배포 전·후를 포함한 전체 수명 주기 동안 지속적으로 테스트되어야 하며, 조직은 명확한 수용 기준을 설정하여 시스템 성능을 평가하고 예기치 않은 변화나 부작용을 모니터링해야 함

- ⑤ AI 시스템의 수명 주기 전반에 걸친 의미있는 인간 통제 보장
  - 조직 내 각 AI 시스템과 제품에 대해 책임질 수 있는 역량 있는 담당자를 지정하여, 필요할 경우 개입할 수 있도록 함으로써 의도치 않은 결과의 가능성을 줄여야 함
- ⑥ 최종 사용자(end-user)에게 AI를 활용한 결정, AI와의 상호작용 방식, AI 생성 콘텐츠에 대한 정보 투명하게 공개
  - 이를 통해 사용자 및 커뮤니티와의 신뢰를 구축하며, AI 시스템, 관련 이해관계자, 사용 기술을 고려하여 가장 적절한 공개 방식을 결정해야 함
- ⑦ AI 시스템의 영향을 받는 사람들이 AI 사용이나 결과에 대해 이의를 제기할 수 있는 절차 수립
  - 조직은 AI 시스템의 영향을 받는 이해관계자들이 조직의 AI 사용 방식에 대해 문제를 제기하고, AI가 생성한 출력물이나 결정에 대해 이의를 제기할 수 있는 프로세스를 마련해야 함
- ⑧ 데이터, 모델, 시스템에 대해 AI 공급망 전반의 다른 조직과 투명하게 공유하여 위험을 효과적으로 해결할 수 있도록 지원
  - AI 개발자와 배포자는 투명성을 유지하며, 안전하고 책임감 있는 AI 관행을 준수하면서, AI 시스템의 구성, 구축 방식, 위험 관리에 필요한 정보를 충분히 확보해야 함
- ⑨ 제3자가 안전장치 준수 여부를 평가할 수 있도록 기록 보관 및 유지
  - 조직은 사용 중인 각 AI 시스템에 대한 최신 조직 전체 인벤토리를 작성 및 유지해야 하며, 해당 기록은 가이드라인의 준수를 입증할 수 있어야 함
- ⑩ 안전성, 다양성, 포용성, 공정성에 중점을 두고 이해관계자들의 요구와 상황에 대해 평가·소통해야 함
  - 이러한 소통은 조직 및 시스템 차원에서 AI 시스템의 전 과정에 걸쳐 이루어져야 함

4. 결론 및 전망

▌제안서와 자발적 AI 안전 표준은 AI 모델 및 시스템을 개발하는 조직에 규제적 명확성과 확실성을 제공

하고, 이러한 신기술의 안전한 활용을 지원하려는 호주 정부의 의지를 나타냄

- 제안서는 고위험 환경에서 AI 안전장치를 도입하기 위한 세 가지 주요 접근 방안을 제시하고 있음
- 모든 AI 개발 및 배포 관련 조직은 제안서의 내용을 숙지하고 이에 대한 의견을 검토할 필요가 있으며, 특히 리스크 관리 절차와 데이터 거버넌스 조치를 정기적으로 검토하고 강화하는 것이 중요

▌한편, 전문가들은 AI 공급망에 있는 모든 조직에 자발적 안전장치를 사전에 숙지하고, 향후 도입될 필수 규제에 대비하여 이를 실질적으로 적용하는 준비를 할 것을 권장

- 필수 안전장치는 아직 협의 중이지만, 조직들은 자발적 안전 표준을 미리 도입함으로써 AI 혁신을 책임감 있게 관리할 내부 역량을 선제적으로 구축하는 것이 유리할 것
- 자발적 AI 안전 표준은 고위험 환경에 국한되지 않고, 전반적으로 AI의 안전하고 책임있는 사용을 보장하기 위한 모범 지침을 제공하고 있음
- 따라서 단기간 내에 자발적 안전장치를 도입한 조직은 향후 시행될 규제 준수 의무에 비교적 수월하게 적응하고 국제 기준과의 일관성을 유지할 수 있을 것으로 예측
- 만약 필수 안전장치가 법적 규제로 시행되지 않더라도, 이는 국제적 모범 관행을 반영하고 있어 안전하고 책임 있는 AI 개발 및 배포를 위해 준수할 필요가 있을 것
  - 안전 표준의 채택은 AI 관련 위험과 피해로부터 개인, 지역사회 및 사회 전반을 보호하려는 조직의 의지를 나타낼 수 있음
  - 이에 따라 이러한 관행을 도입함으로써 소비자 신뢰를 구축하고 시장에서 경쟁 우위를 확보하는 데 기여할 수 있을 것으로 전망

출처 |

1. DISR, The 10 Guardrails, 2024.9.5.
2. DISR, Voluntary AI Safety Standard, 2024.9.5.
3. DISR, Introducing mandatory guardrails for AI in high-risk settings: proposal paper, 2024.10.4.
4. DISR, Safe and responsible AI in Australia: Proposals paper for introducing mandatory guardrails for AI in high-risk settings, 2024.9.
5. Global Compliance News, Australia: New safety measures introduced for AI, 2024.9.17.
6. Herbert Smith Freehills, Australia releases new mandatory guardrails and voluntary standards on AI – what you need to know, 2024.9.9.
7. Maddocks, Guard(rail)ing the development and deployment of AI: the Australian Government's proposal, 2024.9.16.
8. Minister for Industry and Science, The Albanese Government acts to make AI safer, 2024.9.5.
9. Practical Law, Australian Government consults on proposed guardrails for high-risk AI and releases Voluntary AI Safety Standard, 2024.9.5.

2024
개인정보보호 월간동향분석
발간 목록

No.	호수	제목
1	1월 1호	EU 데이터법(Data Act) 주요 내용 분석 및 시사점
2	1월 2호	EU 내 메타의 무광고 유료 서비스 모델의 개인정보 침해 이슈 분석
3	2월 1호	미국 주(州) 개인정보 보호법에 대한 평가 및 분석
4	2월 2호	DPO 지정 및 역할에 대한 CEA 2023 조사 분석
5	3월 1호	미국 백악관의 정부 데이터 및 민감 개인정보보호를 위한 행정명령 분석
6	3월 2호	EDPB, GDPR 주 사업장에 관한 성명 발표
7	4월 1호	생체인식정보에 대한 개인정보보호 이슈
8	4월 2호	미국 AI 에듀테크 시장 관련 개인정보보호 규제 현황 및 고려사항
9	5월 1호	미국 APRA(American Privacy Rights Act) 주요 내용 분석
10	5월 2호	EDPS 2023 연례보고서 분석
11	6월 1호	중국-미국 간 데이터 관련 이슈
12	6월 2호	EU AI 법 및 GDPR의 상관관계 분석
13	7월 1호	애플의 '애플 인텔리전스' 출시 및 EU 규제 이슈
14	7월 2호	EU 기본권청, DPA의 GDPR 집행 이슈 및 모범사례 공개
15	8월 1호	EU GDPR과 LLM간 관계성 분석
16	8월 2호	구글, 크롬 서드파티 쿠키 지원 종료 계획 철회
17	9월 1호	X 플랫폼(구 트위터)의 Grok AI 챗봇 관련 GDPR 위반사례 분석
18	9월 2호	LLM 대안으로서의 LAM, 최신 동향과 개인정보보호 이슈
19	10월 1호	슈렘스 사건 등 CJEU의 최근 개인정보보호 관련 판례 분석
20	10월 2호	호주 정부, 고위험 AI 안전장치 제안 협의 및 자발적 AI 안전 표준 발표

2024
개인정보보호 월간동향분석

『2024 개인정보보호 월간동향분석 보고서』는
개인정보보호위원회 출연금으로 수행한
사업의 결과물입니다.

발행

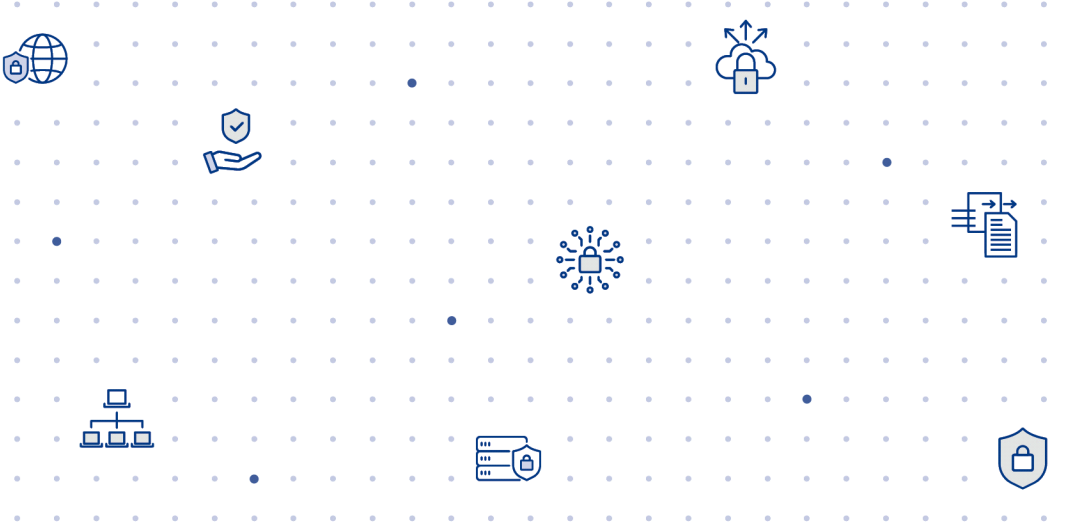
발행일 2024년 11월

발행처 한국인터넷진흥원 개인정보제도팀
전라남도 나주시 진흥길 9
Tel : 061-820-1231

2024
개인정보보호
월간동향분석

2024 Vol.10

PRIVACY REPORT



KISA 한국인터넷진흥원