

2023 Privacy Report

# 개인정보보호 월간동향분석

9월호



2023 Privacy Report

# 개인정보보호 월간동향분석

9월호

1. 미국 데이터 브로커 관련 규제 및 정책 동향
2. 데이터 스크래핑에 대한 12개 개인정보 감독기관의 공동  
성명 발표와 관련 주요 이슈
3. EU 디지털서비스법(DSA)의 개인정보보호 관련 규정

KISA

## 미국 데이터 브로커 관련 규제 및 정책 동향

### [ 목 차 ]

#### 1. 개요

#### 2. 미국의 데이터 브로커 규제 움직임

- (1) 데이터 브로커 현황과 문제점
- (2) CFPB의 브로커 활동 금지 규정 제안
- (3) 상하원의 소비자 권리 강화 법안 발의
- (4) 백악관의 데이터 브로커 관련 원탁회의

#### 3. 평가와 전망

#### 1. 개요

- ▶ 데이터 브로커\*가 개인정보를 수집 및 처리 과정에서 발생하는 각종 개인정보 침해에 대한 우려가 커지면서 미국 행정부와 의회가 문제 해결을 위한 적극적인 대응에 나섬

\* Data broker : 소득, 인종, 정치적 신념, 위치 정보 등 개인 데이터를 공공기록 또는 비공개 방법으로 수집해 제3자에게 판매하거나 라이선스를 부여하는 개인 또는 기업을 의미

- 미국 내 수천 개의 기업형 데이터 브로커가 수십억 개에 달하는 미국인 개인정보 요소를 아무런 통제 없이 구매·집계·공개·판매하고 있는 가운데, 이들 개인정보에 대한 기업 수요가 늘면서 산업이 빠르게 성장
- 데이터 브로커 및 관련 산업의 확산으로 소비자 개인정보를 손쉽게 확보한 기업들은 이를 고객 식별 및 평가 등에 사용해 막대한 수익을 창출하고 있지만, 정작 소비자는 별다른 이익 없이 자신의 개인정보 유출 및 남용 우려만 커지고 있는 상황

- 특히 소비자 개인정보보호를 위한 연방 규정이 존재하지 않아 데이터 브로커 산업에 대한 통제와 규제가 이뤄지지 않아 우려가 더욱 크게 커지고 있음
- ▶ 오래전부터 데이터 브로커가 미국인 개인정보에 미치는 위험에 대한 경고가 계속해서 제기됐지만, 산업 위축에 대한 우려와 업계의 적극적인 로비 등으로 입법이 이뤄지지 않음
- 바이든 대통령이 지난 두 번의 국정 연설을 통해 의회가 포괄적인 연방 개인정보보호 법안\*을 통과시킬 것을 촉구했지만, 아직까지 이행되지 않음
  - \* American Data Privacy and Protection Act
- 지난해 상원에 데이터 브로커를 규제하는 법안이 발의되어 관심이 집중됐지만, 데이터 브로커 산업의 적극적인 로비 등으로 의회를 통과하지 못하고 폐기됨
- '22년 8월 FTC는 개인 건강정보(낙태 기록)를 사용자 동의 없이 판매한 데이터 브로커를 제소했지만, 해당 브로커(Kochava)는 위치 정보를 비식별화해 규정을 준수했다고 맞섰고 결국 소송은 기각됨
- ▶ 하지만, 올해 들어 듀크대학교의 개인 정신건강 정보가 아무 통제 없이 오픈마켓에서 판매·거래·사용된다는 보고서가 발표되자 제도 개선 목소리가 다수 제기됨('23.02.)
  - \* Duke Sanford, 'Data Brokers and the Sale of Americans' Mental Health Data, 2023.2.
- 하원 에너지 및 상업위원회가 복수의 데이터 브로커에 소비자 개인정보 수집과 사용 방법 관련 정보 제공을 요청하는 서한을 발송해 초당적인 조사에 착수('23.04.)
- 상하원 의회도 데이터 브로커를 규제하는 새로운 법률 제정에 나섬
  - 상원은 소비자가 데이터 브로커와 기업을 상대로 개인정보의 수집 중단을 요구할 수 있도록 하는 법안(일명 DELETE Act)\*을 발의('23.06.)
    - \* 개인정보 삭제 및 광범위한 추적 및 교환 제한 법안(Data Elimination and Limiting Extensive Tracking and Exchange Act, DELETE Act)
  - 하원 사법위원회도 데이터 브로커가 연방기관 및 법 집행기관에 개인정보를 판매하는 것을 금지하는 법안을 발의('23.07.)
- 소비자 금융보호국(CFPB)\*은 모든 데이터 기업에 ▲특정 개인정보 판매 금지 ▲민감한 신용 헤더\*\* 데이터 공개 제한 ▲소비자에게 개인정보 판매 이의 제기 권리 부여 등의 새로운 규정 도입 계획을 발표('23.08.)
  - \* Consumer Financial Protection Bureau : 소비자가 은행, 대출업체 및 기타 금융기관으로부터 공정한 대우를 받을 수 있도록 보장하기 위해 설립된 미국 정부 기관
  - \*\* Credit Header Data : 신용보고서에 포함된 이름·주소·전화번호 등 개인식별정보로 기업은 이를 데이터 모델링, 고객 식별 등에 사용하지만, 고객 신용 기록이 아니라는 이유로 규제가 적용되지 않음

- 백악관도 데이터 브로커의 개인정보보호 위협과 이에 대한 정책적 대응을 점검하는 원탁 회의를 개최해 포괄적 개인정보보호 법안 도입을 촉구('23.08.)

## 2. 미국의 데이터 브로커 규제 움직임

### (1) 데이터 브로커 현황과 문제점

- ▶ 데이터 브로커는 다양한 소비자 개인정보(이름, 성별, 나이, 주소, 전화번호, 직업, 소득, 결혼, 자녀, 이메일, 교육수준, 정치 성향, 부동산 등)를 광범위하게 수집·집계
- 정보 수집기술 및 웨어러블 기기 확산으로 개인 구매, 쇼핑 장소, 결제 방법, 건강정보, 실시간 위치 등 더욱 세분화한 개인정보를 수집하고 판매
- 데이터 브로커 산업이 수백만 명 미국인의 프로필을 구축했지만, 이를 통제할 연방 차원의 개인정보보호법이 없어 개인정보 및 시민권, 국가안보에 대한 위협이 증대
- ▶ 미국은 신용기회평등법(ECOA)\*에서 금융기관의 신용평가 및 대출 등에서 차별을 금지하지만, 데이터 브로커는 규정 위반에도 조사·처벌 규정이 없어 방치된다는 지적
  - \* Equal Credit Opportunity Act : 소비자신용보호법 제7조로 대출 신청자의 정당한 권리가 인종, 종교, 피부색, 출신국 등에 따른 차별을 금지함
- 데이터 브로커는 개인정보 사용에서 소비자 공지나 동의를 받지 않고 비밀 알고리즘을 이용해 프로필을 작성하지만, 소비자는 알고리즘으로 결정된 평가 결과에 접근할 수 없는 점 등이 유출 및 남용 우려를 키움
- CFPB 조사 결과, 흑인·라틴계 시민은 백인보다 신용점수가 전반적으로 낮게 나타남
- 하지만 현행법은 규제기관에 브로커의 ECOA 위반 혐의에 대한 조사 권한을 부여하지 않고, 신용 점수 결정에 대한 소비자의 알 권리도 보장하지 않음
- 미국 개인정보보호 옹호론자들은 의회가 포괄적인 연방 개인정보보호법을 도입하고 이를 바탕으로 미국 개인정보보호 규제기관(U.S. Data Protection Agency)을 설립해 데이터 브로커 산업을 규제해야 한다고 강조
- ▶ 버몬트주, 캘리포니아주 등 일부 주에서 데이터 브로커 규제 법안이 도입됐지만, 주마다 규제 편차가 크고, 연방 차원의 브로커 관련 규제가 이뤄지지 않음
- 버몬트주는 2018년 미국 주 가운데 최초로 데이터 브로커 법을 도입해, 매년 규제기관에 등록, 데이터의 수집, 거부, 구매자 자격 증명, 보안 관련 정보 제공을 의무화함

- 캘리포니아주도 2019년 버몬트와 유사한 법을 도입해 데이터 브로커에 규제기관 의무 등록과 소비자에게 자신의 개인정보 판매 거부 방법에 대한 정보를 제공하도록 규정

## (2) CFPB 새로운 규정 도입 제안

- ▶ CFPB는 '23년 8월 데이터 브로커의 소비자 개인정보 거래 비즈니스를 개인 신용점수, 건강·범죄 정보 등 민감한 개인정보를 다루는 감시산업\*에 포함해 규제할 것을 제안
  - \* surveillance industry : 국가안보, 테러, 사회 불안 예방 등을 목적으로 개인 활동이나 통신 정보 등을 수집·분석하는 산업으로 정부 기관 중심에서 점차 민간 기업의 진출이 증가함
- CFPB는 수백만 미국인의 개인정보를 유출, 사이버 공격, AI 챗봇 등 위협에서 보호하기 위해서는 광범위한 데이터 브로커 산업에 대한 통제가 필요하다고 제안 배경을 설명
- 업계는 일부 주에서 제한적으로 시행 중인 데이터 브로커 규제를 미국 전역의 개인정보 구매 및 판매에 대한 통제로 확대하기 위한 강력하고 포괄적인 조치라고 평가
- ▶ CFPB의 제안은 아직 전면 공개되거나 최종 확정되지 않은 단계로 예외 상황을 제외하고는 특정 소비자 정보(소득, 범죄, 결제 등)에 대한 데이터 브로커의 판매를 금지할 방침
- 또한, 데이터 브로커가 주요 신용 평가기관으로부터 사회보장번호, 이름, 주소 등을 구매해 소비자 프로필을 생성하고 이를 판매하는 행위에 제약을 부여할 계획
- CFPB 제안은 공정신용보고법\*을 기반으로 민감한 개인정보를 판매하는 데이터 브로커에 고용 신용조회\*\* 또는 신용 승인\*\*\* 등 정해진 목적으로만 개인정보 판매를 허용
  - \* Fair Credit Reporting Act : 미국 소비자 신용보호법 제6조로 신용조사 기관 및 의료정보 기업은 법에 명시된 목적 이외에는 소비자 개인 정보를 누구에게도 제공하지 못하도록 금지함
  - \*\* employment background checks : 고용 시 신원 조사를 통해 개인의 경력, 학력 등을 확인하고, 이력서의 거짓 여부 및 누락, 범죄 행위 등을 파악하는 행위
  - \*\*\* credit decisions : 신규 또는 추가 대출 시 대출 허용, 한도, 조건 등을 결정하는 단계
- CFPB는 이번 제안이 데이터 브로커 산업의 소비자 데이터의 수집·사용·공유 방식에 대한 광범위한 우려를 해소하고, 관련 데이터 공유가 소수자, 노인, 이민자 등 소수 계층에 더 큰 피해를 주는 불균형 완화에 있다고 강조
  - CFPB 제안은 소규모 비즈니스 그룹을 통한 피드백 수렴을 준비하는 단계에 있으며, 이후 공식 규칙 제정 절차에 따라 내용이 공개될 예정
- ▶ CFPB 외에 연방거래위원회(FTC)도 데이터 브로커 산업 규제를 추진하고 있음
  - FTC 리나 칸 위원장은 지난해 데이터 브로커 산업의 행태를 개인에 대한 지속적인 추적과 일상화된 감시라고 지적하고, 모든 기업이 소비자 개인정보의 수집과 사용 방식을 제한할 수 있는 포괄적 규정 도입을 언급

### (3) 상·하원의 소비자 권리 강화 법안 발의

- ▶ **(상원의 DELETE Act 개요)** '23년 6월 미 상원은 소비자가 데이터 브로커와 기업을 상대로 개인정보 수집 중단을 요구할 수 있도록 하는 법안을 발의
  - 해당 법안은 '개인정보 삭제와 광범위한 추적 및 교환 제한 법안'(약칭 DELETE Act)으로 명명됐고, 데이터 삭제 요구사항 등을 구체적으로 명시
  - 지난해 발의되었던 유사 법안이 회기 내 처리되지 못해 폐기됐지만, 이번 법안(S.3627)은 FTC로부터 받은 피드백을 반영하고 구체적인 집행 메커니즘이 추가됨
  - 법안을 발의한 빌 캐시디(Bill Cassidy)와 존 오소프(Jon Ossoff) 의원은 현 규정은 소비자가 개인정보 삭제를 원할 경우, 각 데이터 브로커에 삭제를 직접 요청해야 해 번거로우며, 다양한 경로를 통해 퍼진 개인정보의 완전 삭제가 불가능하다고 지적
  - 이번 S.3627 법안은 규제당국에 삭제를 명령할 수 있는 권한과 개인정보 수집을 금지하는 추적 금지 목록 작성 권한 부여를 명시
  - 이에 따라, FTC에 ▲데이터 브로커 규제 권한과 ▲등록된 데이터 브로커에게 소비자가 한 번에 일괄적으로 전송하는 '데이터 삭제 요청' 온라인 대시보드 기능 개발 책무를 부여
  - 업계는 이번 법안이 현 상태를 확실히 개선할 수 있다고 평가했고, 소비자 보호 단체들도 법안의 재발의를 환영
- ▶ **(DELETE Act 주요 내용)** S.3627 법안은 ▲데이터 브로커의 연간 등록 ▲중앙집중식 데이터 삭제 시스템 구축 ▲규제기관 집행 ▲규제기관 요구사항 등으로 구성됨
  - **(데이터 브로커의 연간 등록)** 법안 공표 후 1년 이내에 FTC는 데이터 브로커가 준수할 규정을 공개하며, 규정은 다음의 내용을 포함해야 함
    - 데이터 브로커는 법안 공표 후 18개월 이내에 FTC에 등록하며 ▲데이터 브로커의 이름, 주소, URL, 이메일 주소 ▲개인정보 수집 및 사용 중단 요청 조건(방법, 제한 요건 등) ▲수집 정보 유형과 취득 출처 ▲인증 프로세스 준수 여부 등을 공개해야 함
    - FTC는 해당 정보 공개가 공공의 안전이나 복지를 저해하는 경우가 아닐 경우, 다운로드 및 기계 판독이 가능한 형식으로 공개하도록 해야 함
  - **(중앙집중식 삭제 시스템)** 법안 공표 후 1년 이내에 FTC는 온라인 대시보드와 같은 중앙 집중식 삭제 시스템 구축을 위한 규정을 발표해야 함
    - 중앙집중식 삭제 시스템은 ▲합리적 보안 절차와 관행 준수 ▲개인이 한 번의 요청으로 관련 하위 섹션 모든 개인정보 삭제 지원 ▲데이터 브로커 및 계열사가 보유한 모든 개인정보 삭제 등을 구현해야 함



- 중앙집중식 삭제 시스템은 개인이 한 번의 요청으로 모든 개인정보가 삭제할 수 있어야 하며, 이러한 요청을 지원하는 표준화된 양식을 제공해야 함
- 중앙집중식 삭제 시스템은 제출된 모든 정보를 자동으로 해시(hash) 처리하며, 독립적인 해시 레지스트리를 유지할 수 있어야 함
- 중앙집중식 삭제 시스템은 저장된 개별 개인정보를 2년마다 자동 삭제하고, 소비자가 개인정보 삭제를 요청할 경우 FTC는 자동 삭제 기간 정보를 제공해야 함
- FTC는 법안 공표 후 18개월 이내에 추적 금지 목록 규정을 발표해야 하며, 여기에는 삭제를 요청한 개인의 개인정보 수집이나 보유를 금지하는 내용이 포함되어야 함

• **(규제기관 집행)** 불공정한 경쟁, 기만적인 거래행위 또는 관행 등을 다루는 FTC법(Federal Trade Commission Act) 제5조에서 규정한 불법 행위는 규정 위반으로 간주

- FTC는 FTC법의 모든 약관 및 조항을 이번 법안에 동일한 방식, 동일한 수단, 동일한 관할권, 동일한 권한 및 의무로서 적용

▶ **(하원의 관련 법안)** 지난 '23년 7월 19일, 제리 내들러(Jerry Nadler), 워렌 데이비슨(Warren Davidson) 등 8인의 공화당·민주당 하원의원은 연방기관과 법 집행기관의 데이터 브로커로부터의 개인정보 구매를 금지하는 법안(H.R. 4639)\*을 재발의해 하원 사법위원회를 통과시킴

\* Fourth Amendment is Not for Sale Act(수정헌법 제4조 판매금지법): '21년 처음 발의되었으나 제117대 회기 내 제정되지 못한 법안으로 일부 수정된 법안이 지난 7월 재발의되어 사법위원회 통과

※ 하원 사법위원회 통과에 보조를 맞추어 상원에서도 약 일주일 뒤인 7월 27일 론 와이든(Ron Widen)위원을 중심으로 유사 법안(S.2576)을 재발의

- 의원들은 법 집행기관의 소비자 개인정보 구매는 영장을 통해서만 소비자 개인정보 확보가 가능하도록 한 수정헌법 제4조를 위반한다고 지적하고, 미국인의 권리 회복과 무분별한 개인정보 수집을 막기 위한 법안 도입에 나선다고 강조
- 하원은 동 법안 재발의 일주일 전 승인한 국방 지출 승인안에서도 국방부의 데이터 브로커 개인정보 구매를 제한하는 등 데이터 브로커 규제를 강화하는 일관된 모습을 견지
- 이번 법안은 데이터 브로커 규제에 대한 양당의 초당적 합의를 바탕으로 하고 있으며 상원과도 동시에 추진하고 있어 빠른 입법화가 가능할 것이라는 전망이 제기됨

#### (4) 백악관 원탁회의

- ▶ '23년 8월 백악관은 데이터 브로커 산업이 개인정보를 통해 수익을 창출하는 방법과 잠재적 소비자 피해 우려에 대한 정부 대응에 대한 의견수렴을 위해 원탁회의를 개최



- 원탁회의는 백악관 과학기술정책실, 국가경제위원회, 소비자금융보호국, 연방거래위원회, 법무부 주최로 다양한 시민단체, 개인정보보호 전문가, 정책 입안자들이 대거 참여
- 원탁회의가 개최된 8월 16일, CFPB는 모든 데이터 기업에 특정 개인정보 판매 및 공개를 금지하고 소비자에게 개인정보 판매 이의 제기 권리를 부여한 규정 도입을 발표
- CFPB 계획을 계기로 미 행정부는 데이터 브로커에 대한 규제와 감독을 강화하고, 그로 인한 피해를 줄이기 위한 법적 권한 사용을 약속
- ▶ 과학기술정책실 아라티 프라브하카르(Arati Prabhakar) 실장은 바이든 대통령이 미국인 개인정보 수집을 제한하기 위해 데이터 기업에 더욱 강력한 개인정보보호 조치를 요구했다고 공개
- 참가자들은 원탁회의에서 데이터 브로커의 관행이 일상적 미국인에게 미치는 피해와 위험에 대한 현황과 우려를 공유
- 주요 논의 주제로는 ▲세부적인 민감 데이터의 은밀한 수집, 사용, 판매 ▲흑인과 유색인종의 주택 및 경제 기회를 차단하는 신용점수 평가 ▲인지적 취약성을 가진 개인을 대상으로 한 약탈적 사기 ▲성폭력 등 개인 안전에 대한 위험 증가 ▲데이터 브로커에 대한 관리 부재 등의 문제가 부각
- ▶ 원탁회의에서는 참석자들이 비동의, 무분별한 수집, 오래된 개인정보로 인한 피해, 소외 계층에 대한 피해 등 다양한 문제점에 대해 논의
- 참석자들은 데이터 브로커가 위치정보, 건강정보 등을 대량으로 구매 및 확보하는 방법을 공유하고, 이를 당사자가 알지 못하거나 동의하지 않은 경우가 빈번하다고 지적
- 또한, 최근 인공지능의 발전으로 데이터 브로커가 개인의 라이프 스타일, 욕구, 약점 등을 추론하는 능력이 급속도로 확대되고 있으며, 무분별한 개인정보 수집이 데이터 브로커의 성장을 부추긴다고 우려
- 광고주, 금융기관, 고용인, 집주인, 사기꾼 등 다양한 집단이 데이터 브로커와 거래를 통해 개인정보를 보유하며, 이 때문에 개인과 집단의 피해가 급속도로 커진다고 진단
- 부정확하거나 오래됐거나 목적에 맞지 않는 민감한 개인정보의 유통으로 신용 및 주택 대출 신청 등에서 많은 시민의 피해를 발생하고 있다는 지적 또한 제기
- 원탁회의는 데이터 브로커 경제가 신용 분류(Credit Underwriting), 보험, 주택, 고용, 광고 등에서 차별적 관행을 조장하고, 소외되고 취약한 계층을 배제하는 불균형 피해를 지속 시킨다고 강조

- 여성의 경우, 데이터 브로커가 판매하는 위치정보는 여성들이 낙태 등을 위해 의료 서비스를 이용하는 것을 방해\*한다고 지적

\* 미국에서는 '22년 6월 도브스 대 잭슨 여성 건강 기구 사건에 대한 연방 대법원 판결로 지난 50여 년간 사생활 권리로 인정받았던 여성의 낙태 권리가 위법화 됨. 이에 따라 여성들은 낙태를 위해 의료시설을 방문하는 것과 관련한 위치정보 노출을 극히 꺼리게 됨

- ▶ 업계는 원탁회의와 CFPB 제안 발표 등이 바이든 정부가 데이터 브로커 산업에 대해 더욱 강력한 규제를 도입하려는 가장 최근의 징후라고 평가

- 바이든 행정부는 기업의 개인정보 수집·사용·공유를 명확한 기준에 따라 제한함으로써 악의적인 데이터 사용 관행을 차단하면, 시민은 자신의 데이터가 사용되는 방식에 대해 더 많은 선택권을 갖게 될 것으로 기대

### 3. 평가와 전망

- ▶ **(근원적 문제)** 미국에서 데이터 브로커에 대한 우려가 확산되면서, 일각에서는 그들이 사용하는 개인정보 대다수가 정부로부터 확보한 것이라는 근원적인 문제를 제기

- 여권 갱신부터 중소기업 대출에 이르기까지 다양한 연방 서비스를 제공하는 사이트 Login.gov\*는 미국 국민들이 사회보장번호와 주(州) ID를 기반으로 가입하고 접속

\* 미국인들이 연방정부가 제공하는 전자정부 서비스를 이용하기 위해 접속하는 Single Sign-On 웹사이트. '17년 4월 기존 Connect.Gov를 대체해 서비스를 가동하기 시작. 20여 개 이상의 연방정부 기관에서 제공하는 공공 서비스를 연결해 제공

- 그러나 정작 Login.gov를 운영·관리하는 연방 총무청(GSA) 등 정부기관은 '74년에 제정된 개인정보보호법(Privacy Act)\*으로 인해 해당 개인정보에 접속할 수 없음

\* Privacy Act of 1974은 개인정보 기록에 대해 연방정부 기관 간 사용 및 공유를 제한

- 반면, Login.gov 사이트 가입 시 사기 방지를 위해 가입자에 대한 신원 확인을 맡고 있는 데이터 브로커는 개인정보보호법에 민간 기업에 대한 규정이 없는 허점을 이용해 수백만 명의 미국인 프로필을 생성해 미국 정부에 재판매하면서 급성장하고 있음

- 이 같은 상황은 Login.gov뿐만 아니라 노동부가 제공하는 주(州) 실업 보험 프로그램 사이트 등 다양한 정부의 웹 서비스 가입 과정에서 발생하고 있는 실정

- ▶ **(비판)** 데이터 브로커 규제를 요구하는 진영은 정부가 브로커들에게 신원 확인 업무를 맡겨 소비자 개인정보 수집이 가능하게 해주고 행정 및 사법 집행을 위해 데이터 브로커가 처리한 개인정보를 구매해 데이터 브로커 산업을 키우고 있다고 지적

- 연방기관들이 데이터 브로커에 의존하지 않을 대안으로 FBI가 통제하는 등록번호를 통해 민간 비영리단체 NLETS\*가 관리하는 시스템의 대규모 민간 개인정보 데이터베이스를 연방 기관들이 활용하는 방안이 있으나 FBI가 이를 거부하고 있어 쉽지 않은 상태

\* National Law Enforcement Telecommunication System

- ▶ **(전망)** 데이터 브로커 업계의 확산으로 ▲무분별한 개인정보 수집·처리·판매 ▲소비자에 대한 잘못된 정보로 인한 피해 ▲개인 안전 및 국가 안보의 위험도 증가 등이 고조되고 있어 문제 해결을 위한 다양한 입법 활동이 전개
- 미국 백악관의 지원 속에 의회는 『연방 개인정보보호법』, FTC를 통해 데이터 브로커에 대해 관리·감독을 강화하는 『개인정보 삭제 및 광범위한 추적 및 교환 제한 법』(DELETE Act), 연방기관의 데이터 브로커로부터의 데이터 구매를 금지하는 『수정헌법 제4조 판매 금지법』의 조속한 입법화를 추진할 전망

#### Reference

1. Bill Cassidy 상원의원 홈페이지, Cassidy, Ossoff, Trahan, Edwards Reintroduce Bill to Protect Americans' Online Privacy and Data, 2023.06.22
2. CNN, US watchdog teases crackdown on data brokers that sell Americans' personal information, 2023.08.15.
3. Cyberscoop, Legislation preventing data broker sales to government agencies moves forward, 2023.07.19.
4. Cyberscoop, White House hosts roundtable on harmful data broker practices, 2023.8.15
5. White House, Readout of White House Roundtable on Protecting Americans from Harmful Data Broker Practices, 2023.08.16.
6. Politico, Data brokers raise privacy concerns, get millions from the federal government, 2022.12.21.
7. Ron Wyden 상원의원 홈페이지, Wyden, Paul and Bipartisan Senators Reintroduce the Fourth Amendment is Not for Sale Act, 2023.07.27.

# 데이터 스크래핑에 대한 12개 개인정보 감독기관의 공동 성명 발표와 관련 주요 이슈

## [ 목 차 ]

### 1. 개요

### 2. 데이터 스크래핑 관련 주요 이슈

- (1) 12개국 개인정보 감독기관의 공동 성명 발표
- (2) EU GDPR과 데이터 스크래핑
- (3) 데이터 스크래핑에 대한 소송 사례

### 3. 시사점 및 전망

### 1. 개요

▶ 생성형 AI 모델 출시가 증가하면서, AI 학습을 위한 데이터 스크래핑(Data Scraping)이 새로 주목받으며, 개인정보보호, 지식재산권, 라이선스 등에서 새로운 이슈를 야기

\* 웹 스크래핑(web scraping)으로도 불리며, 웹 사이트 정보를 컴퓨터 내 스프레드시트나 로컬 파일로 가져오는 프로세스를 의미하며, 웹에서 데이터를 가져오는 가장 효율적 방법 중 하나로 평가됨

- '23년 8월 영국 ICO, 캐나다 OPC, 홍콩 OPCPD 등 12개국\* 개인정보 감독기관은 데이터 스크래핑에 대한 우려를 수용해 소셜 미디어 플랫폼에 사용자 공개 게시물이 스크랩되지 않도록 보호할 것을 촉구하는 공동 성명을 발표<sup>1)</sup>

\* 호주, 캐나다, 영국, 중국, 스위스, 노르웨이, 뉴질랜드, 콜롬비아, 저지, 모로코, 아르헨티나, 멕시코

1) OAIC, Global expectations of social media platforms and other sites to safeguard against unlawful data scraping, 2023.8.24.  
<https://www.oaic.gov.au/newsroom/global-expectations-of-social-media-platforms-and-other-sites-to-safeguard-against-unlawful-data-scraping>

- 12개 개인정보 감독기관은 공동 성명문에서 잇따른 생성형 AI 모델 출시와 더 많은 데이터 세트 확보 경쟁이 스크래핑 기술의 광범위한 확산을 초래한다고 우려하고, 인터넷 게시물 무단 스크래핑은 대다수 국가에서 법적 책임이 따른다고 경고
- 특히, 인터넷에 ▲공개사용(publicly available) ▲공개 액세스(publicly accessible) ▲공적 속성(public nature) 등으로 표현된 소비자 개인정보는 데이터 보호 및 개인정보보호법 적용을 받아, 해당 정보를 스크랩하는 기업과 개인은 법률을 준수할 책임이 있다고 강조
- ▶ 과거부터 논란이 되어 왔던 데이터 스크래핑은 최근 광범위한 대규모 스크래핑이 가능해져 소셜 미디어 플랫폼의 개인정보 무단 추출 및 사용, 허술한 개인정보보호 관행에 대한 우려가 증폭되고 있는 상황
- '18년 영국에서 페이스북-케임브리지 애널리티카 정보 유출 사고\*가 공개되면서 소셜 미디어 플랫폼 기업의 데이터 사용 관행이 사회적 문제로 부상
- \* 영국 정치컨설팅 기업 캠브리지 애널리티카가 '16년부터 페이스북 가입자 프로필을 소비자 동의 없이 수집해 정치적 광고 등에 무단 사용한 사실이 공개됨
- '22년 EU는 페이스북에 데이터 스크래핑 관련 불완전한 제품 설계로 5억 3,000만 명에게 피해를 준 혐의로 2억 7,500만 달러의 과징금을 부과했고, 현재 법정 다툼이 진행 중
- ▶ 데이터 스크래핑을 둘러싼 소셜 미디어 플랫폼, 규제기관, 소비자 간 갈등이 고조되어 소송 제기가 늘고 있으며, 논란 해소를 위한 규정 및 법률 정비가 논의가 확산함
- '23년 6월 캘리포니아주에서 오픈 API의 생성형 AI 모델인 챗GPT(ChatGPT)를 상대로 인터넷 공간의 방대한 개인정보를 무단 스크랩해 학습한 혐의로 집단 소송이 제기됨
- EU에서는 소비자 개인정보를 수집해 개인을 모니터링 및 프로파일링하고 이를 통해 소비자 식별까지 진행한 사례(Clearview AI)가 등장해 당국의 단속을 받음
- 데이터 스크래핑은 사용자의 개인정보보호권, 라이선스 및 오픈 소스 문제, 지식재산권 부문과 얽히면서 갈등이 고조되고 있음

## 2. 데이터 스크래핑 관련 주요 이슈

### (1) 12개국 개인정보 감독기관의 공동 성명

- ▶ 12개 개인정보 감독기관은 데이터 스크래핑이 인터넷에서 방대한 분량의 개인정보를 수집·처리에 점점 더 많이 사용된다고 평가하고 악용 가능성도 커졌다고 진단

- 특히 제3자 웹 사이트에 개인정보 재판매를 통한 수익 창출이 활발해지면서 개인정보에 대한 사적 분석, 악용 목적의 정보 수집 등 개인정보보호 문제가 심각해졌다고 지적
  - 이러한 우려는 소셜 미디어 애플리케이션과 공개접속이 가능한 개인정보를 호스팅하는 웹 사이트에서 주로 이뤄진다고 진단
- ▶ 12개국 감독기관은 데이터 스크래핑이 개인정보를 수집하고 처리하는 기술 발전으로 개인정보 침해에 대한 우려가 더욱 커졌다고 강조
- 데이터 스크래핑이 취급하는 개인정보는 대부분 법의 보호를 받아 개인정보보호 의무가 부여되고, 보호 의무는 해당 정보가 공개 액세스 여부와 관계없이 적용된다고 지적
  - 공개 액세스가 가능한 개인정보를 호스팅하는 웹 사이트는 다양한 유형의 데이터 스크래핑 적법성을 신중히 고려해야 하고, 불법 데이터 스크래핑으로부터 개인정보를 보호할 조치를 도입해야 한다고 권고
- ▶ **(핵심 사항)** 12개 감독기관은 공동 성명에서 **4개 핵심 사항**을 제시
- ① 공개 액세스가 가능한 개인정보는 대부분 관할권에서 데이터 보호 및 개인정보보호법이 적용됨
  - ② 소셜 미디어 기업과 공개 액세스가 가능한 개인정보를 호스팅하는 웹 사이트 운영자는 데이터 보호 및 개인정보보호법에 따라 불법 데이터 스크래핑으로부터 개인정보를 보호할 의무가 있음
  - ③ 대량의 개인정보를 수집하는 데이터 스크래핑 행위는 다수의 관할권에서 개인정보 침해에 해당할 수 있음
  - ④ 사용자는 데이터 스크래핑으로부터 개인정보를 보호할 수 있어야 하며, 소셜 미디어 기업은 사용자가 개인정보를 보호받으면서 서비스를 이용할 수 있도록 지원해야 함
- ▶ **(성명 목적)** 12개 감독기관은 이번 성명이 ▲개괄적인 데이터 스크래핑의 개인정보보호 위험 설명 ▲불법 데이터 스크래핑으로부터 개인정보보호 방법 ▲데이터 스크래핑에서 개인정보 위험을 최소화하기 위한 개인적 조치 등을 제시하기 위한 것이라고 설명
- 특히, 웹 사이트에서 개인정보를 이용하고 게시하는 소셜 미디어와 개인의 개인정보보호 지원에 초점을 맞췄다고 강조
  - 12개 감독기관은 성명에서 제시한 방법이 일반적 글로벌 개인정보보호 원칙과 관행을 반영하며, 개인정보 데이터 스크래핑을 방지하고 개인정보에 미치는 영향을 완화하도록 설계됐다고 설명

- ▶ **(개인정보보호 위험)** 각국 개인정보 감독기관들은 최근 들어 소셜 미디어 및 기타 웹 사이트의 대량 데이터 스크래핑에 대한 보고가 증가하고 있다고 언급
  - 이로 인해 ▲표적화된 사이버 공격 ▲신원사기 ▲개인에 대한 모니터링·프로파일링·감시 ▲개인정보의 불법 사용 ▲동의하지 않은 직접 마케팅 또는 스팸 악용 등의 위험이 커짐
  - (표적화된 사이버 공격) 가령, 해킹 포럼\*에서 수집된 신원이나 연락처 정보는 외부 공격자가 표적 공격 또는 피싱에 사용될 수 있음
    - \* hacking forum: 해킹 관련 문화, 기법, 사이버보안 등에 대한 토론을 벌이는 웹사이트. 최근에는 불법으로 해킹한 정보를 공유 및 거래하는 등의 온라인 범죄의 온상으로 변질
  - (신원사기) 스크랩된 개인정보는 사기 대출, 허위 신용카드 신청, 가짜 소셜 미디어 계정 생성 등 개인 사칭에 사용될 수 있음
  - (개인 프로파일링 및 감시) 스크랩된 개인정보는 안면인식 데이터베이스와 결합 등을 통해 개인에 대한 프로파일링 생성이나 이를 활용한 감시 등에 사용될 수 있음
  - (개인정보의 불법 사용) 스크랩된 개인정보는 해외 정부 또는 정보기관에서 정치적 목적 등으로 불법 사용될 수 있음
  - (직접 마케팅 또는 스팸 악용) 스크랩된 개인정보는 동의하지 않은 직접 마케팅이나 스팸 등에 악용될 수 있음
- ▶ 개인이 알지 못하는 사이에 개인정보가 봇(Bot) 등을 통해 스크랩되면 개인은 자신의 개인정보에 대한 통제권을 상실하게 되고 사용자가 예상하지 못한 목적으로 사용됨
  - 이는 소셜 미디어와 웹 사이트에 대한 신뢰를 떨어뜨려 디지털 경제에 악영향을 미치고, 사용자가 소셜 미디어 계정에서 개인정보를 삭제해도 기존에 수집된 개인정보는 계속 사용·공유될 가능성이 커 개인의 온라인 평판에 대한 개인 통제를 제한
- ▶ **(불법 데이터 스크래핑으로부터 개인정보보호)** 소셜 미디어와 웹 사이트는 불법적인 개인정보 스크래핑으로부터 개인정보를 보호할 의무가 있음
  - 공개 액세스가 가능한 개인정보에서 가치를 추출하고 스크래핑하는 기술이 발전하고 있어 스크래핑 이용 기업에 더 적극적인 개인정보보호 책임이 요구됨
  - 하지만 데이터 스크래핑 관련 모든 잠재적 피해를 완벽히 보호할 수 있는 안전장치는 없으므로, 소셜 미디어와 웹 사이트는 위험 완화를 위해 다층적 기술과 절차적 통제를 구현해야 함
  - 이러한 통제는 정보 민감도에 비례하는 접근이 필요하고, 다음의 사항들을 포함해야 함



- ① 불법 스크래핑 활동을 방지하고 적극적으로 대응하기 위해 조직 내에 관련 활동을 모니터링하고 식별하고 통제하기 위한 팀이나 특정 역할을 지정
- ② 한 계정이 다른 계정 프로필에 하루에 방문할 수 있는 횟수나 시간을 제한하고, 비정상적인 활동이 감지되면 액세스를 제한
- ③ 새로운 계정 생성 후 얼마나 빠르고 적극적으로 다른 사용자를 찾는지 모니터링하고, 비정상적으로 빠른 활동이 감지되면 불법 사용 징후로 파악
- ④ 개인정보 스크랩 봇의 활동 패턴을 식별해 사전 탐지를 구현하고, 여러 위치에서 동일 자격 증명으로 접속하는 IP 사용그룹을 탐지
- 이를 위해서 캡차\* 등 봇을 탐지할 수 있는 도구를 도입하고, 데이터 스크래핑 활동이 식별되는 IP 주소는 신속하게 차단

\* CAPTCHAs : 사용자가 사람인지 자동화된 프로그램(봇)인지를 테스트하는 프로그램

- 데이터 스크래핑이 의심되거나 확인된 경우, 이를 금지하는 정책을 적용하고 ▲중단 서한 발송 ▲스크랩된 정보의 삭제 요청 ▲삭제 확인서 확인 등 조치를 적용
- 데이터 스크래핑이 개인정보 침해에 해당하는 관할권에서는 필요에 따라 피해를 본 개인 및 개인정보 감독기관에 통지
- 이러한 보안 제어 외에도 소셜 미디어 및 웹 사이트는 사용자가 개인정보를 보호받는 환경에서 서비스를 이용할 수 있도록 지원해야 함
  - 이를 위해 소셜 미디어 및 웹 사이트는 사용자가 플랫폼 사용과 개인정보 공유에서 정보를 기반으로 결정할 수 있도록 충분한 정보를 제공해야 함
- 데이터 스크래핑 방지 조치가 개인정보 처리와 관련된 경우, 소셜 미디어와 웹 사이트는 해당 처리가 데이터 보호 및 개인정보 보호법 요건을 준수하는지 확인해야 하고, 해당 기업은 투명성 보장을 위해 조치 내용을 사용자에게 알려야 함
- 데이터 스크래핑 위협이 점점 커지는 특성을 고려해, 소셜 미디어와 웹 사이트는 악의적 또는 비승인 행위자가 플랫폼에 가하는 새로운 보안 위험과 위협을 지속 모니터링하고 민첩하게 대응해야 함
  - 안전장치는 정기적으로 스트레스 테스트와 업데이트로 효과를 유지해야 하고, 소셜 미디어와 웹 사이트는 스크래핑 행위 관련 지표를 수집·분석해 보안 제어 프레임워크에서 개선이 필요한 부분을 파악하고 알려야 함

▶ **(데이터 스크래핑에서 개인정보 위험을 최소화하는 개인적 조치)** 이상의 보안 제어로 데이터 스크래핑 위험을 완화할 수 있지만, 100% 개인정보 안전을 보장할 수는 없어 사용자는 온라인에서 공유하는 개인정보가 위험에 처할 수 있다는 점을 유념해야 함

- 사용자는 ▲소셜 미디어와 웹 사이트가 제공하는 개인정보보호 및 개인정보 공유 방법에 대한 정보 숙지 ▲공유 개인정보 정보의 양과 종류를 고려 ▲개인정보보호 설정에 대한 충분한 이해와 관리 등을 고려해야 한다고 권고
- ▶ 아직 각국 규제당국과 개인정보 감독기관은 AI 학습에 사용되는 데이터 스크래핑을 개인정보보호 위협으로 직접 언급하지는 않은 상황
- 다만, 사용자 동의 없는 개인정보를 통해 학습된 생성형 AI 모델은 표적화된 사이버 공격, 신원 사기 등 다양한 개인정보보호 위협을 초래한다고 경고하는 단계
- 하지만, 데이터 스크래핑으로 개인정보가 해외 정부나 정보기관에 유출될 경우, 국가안보 위협이 커지고, 개인 프로파일링 및 감시에 악용될 수 있다는 우려가 점차 증가
- ▶ 12개국 개인정보 감독기관은 공동 성명 발표 후 페이스북 등 주요 소셜 미디어 기업에 요구사항을 전달하고 피드백을 요구해 데이터 스크래핑 우려가 업계 전반으로 확대됨
- 피드백을 요구받은 기업은 알파벳(유튜브), 바이트댄스(틱톡), 메타(인스타그램, 페이스북, 스레드) 마이크로소프트(링크드인), 시나(웨이보), 엑스(트위터) 등임
- 개인정보 감독기관은 소셜미디어 기업에 요구사항을 전달받은 지 한 달 이내에 당국의 우려와 요구에 어떻게 대응할 것인지에 대한 답변을 요구

## (2) EU GDPR과 데이터 스크래핑

- ▶ EU 개인정보보호 전문가들은 데이터 스크래핑이 생성형 AI 모델 출시가 줄 이으면서 다시 대중의 관심사로 떠올랐다고 평가하고, 데이터 스크래핑과 GDPR 연관성에 주목
- GDPR은 데이터 스크래핑의 적법성을 명시적으로 다루지 않지만, 데이터 스크래핑을 통한 정보 수집을 컨트롤러 또는 프로세서가 다른 수단으로 수집한 개인정보 처리와 유사하게 취급
- 따라서, 기업은 데이터 스크래핑으로 수집한 개인정보를 처리할 수 있는 합법적 근거가 있어야 하고, 해당 개인정보보호와 관리에 필요한 기술·조직적 안전장치를 확보해야 함
- 동시에, GDPR 제5조\*에 명시된 개인정보보호 원칙을 준수할 의무가 부여됨
- \* 개인정보는 정보 주체에 대해 적법, 공정, 투명하게 처리되어야 하며, 구체적, 명시적, 적법한 목적을 위해서 필요한 정도로만 최소로 수집되어야 한다는 등의 원칙을 규정
- 전문가들은 이러한 GDPR 규정에도 불구하고 기업이 개인정보 스크래핑을 수행할 때 특정한 개인정보보호 문제가 발생하고, 위험도가 높아지고 있다고 우려

- ▶ 데이터 스크래핑의 GDPR 준수에서 논란이 되는 것은 개인정보 처리에서 특정 측면을 정보 주체에 공지하도록 한 GDPR 제13조, 제14조임
- GDPR 제13조가 규정한 정보 주체에 공지 의무는 개인정보 주체로부터 직접 개인정보를 수집한 경우에 적용되고, 스크래핑처럼 개인정보를 간접적으로 수집한 경우에는 GDPR 제14조가 적용됨
- GDPR 제14조는 제13조에서 공지하도록 한 정보를 추후 정보 주체에 제공토록 규정하고 3가지 사례\*를 제시
  - \* ▲개인정보 취득 후 늦어도 1개월 후 ▲정보 주체와 첫 커뮤니케이션을 하는 시점 ▲(다른 수신자에게 제공할 계획인 경우) 개인정보가 처음 공개되는 시점으로 각각 규정
- 위 규정과 동시에, GDPR 제14조는 불가능하거나 불균형적 노력이 필요할 때는 정보를 제공하지 않아도 된다는 예외 규정을 명시
- 데이터 스크래핑을 수행한 기업이 수많은 정보 주체에 공지 정보를 제공하는 것이 막대한 비용·시간이 드는 ‘불균형적 노력’에 속해 GDPR 규정 적용 면제에 해당하는지를 둘러싸고 이견이 존재
- 이와 관련해 영국 개인정보 감독기관(ICO)은 ‘불가능성(Impossibility)’과 ‘불균형적 노력(Disproportionate effort)’을 판단 지침으로 제시
  - (불가능성) 기업에 개인정보 주체 연락처가 없고 이를 확보할 수 있는 합리적 수단이 없는 경우에 적용
  - 하지만, 기업이 정보 주체의 세부 정보 확보가 가능한지를 확인하는 조치를 하지 않았을 경우, 해당 규정을 적용할 수 없도록 함
  - (불균형적 노력) 정보 주체에 연락하는 데 필요한 노력과 처리가 개인에게 미칠 수 있는 잠재적인 효과와 비교해 과도할 때 적용

### (3) 데이터 스크래핑에 대한 소송 사례

- ▶ '23년 6월 캘리포니아 북부지방법원에 오픈AI(Open AI)와 마이크로소프트가 생성형 AI 모델 학습에서 수백만 명에 달하는 인터넷 사용자 개인정보를 동의 없이 사용해 개인정보보호 권리를 침해했다는 집단 소송이 제기됨
- 원고는 오픈AI와 MS가 소셜 미디어, 블로그 게시물, 기타 웹 사이트 개인정보를 대규모 스크래핑하고 이를 이용해 자사 AI 모델을 학습시킴으로써 인터넷 사용자의 개인정보를 침해했다고 주장

- 또한, 원고는 피고 기업이 의도적으로 챗GPT(ChatGPT) 플러그인으로 연결된 컴퓨터에 무단 접속해 정보를 획득해 컴퓨터 사기 및 남용방지법(CFAA)\*도 위반했다고 주장

\* Computer Fraud and Abuse Act : 1986년에 제정된 미국 사이버 보안법으로 승인 절차 없이 보호된 컴퓨터에 의도적으로 액세스하거나 권한을 초과하여 액세스하는 개인에게 형사 처벌을 부과

- 원고는 피고 기업이 사용자 개인정보가 머신러닝 모델과 생성형 AI 도구 훈련에 사용될 수 있다는 사실을 적절히 공개하지 않았다고 주장

▶ 여러 혐의 가운데 데이터 스크래핑이 사용자의 개인정보보호 권리를 침해했다는 주장에 대한 법원의 수용 여부를 주목

- 원고는 AI 기업이 머신러닝 학습에서 대규모로 스크래핑한 개인정보를 사용하기 위해서는 사용자의 동의를 얻어야 한다고 주장
- 법원이 원고 주장을 받아들일 경우, AI 기업은 수백만 명에 달하는 인터넷 사용자로부터 소급 동의를 얻어야 해 엄청난 파장이 뒤따를 전망

### 3. 시사점 및 전망

▶ AI를 둘러싼 환경이 빠르게 변화하면서 생성형 AI 모델이 교육 목적으로 인터넷상의 개인정보를 합법적으로 사용해도 되는지에 대한 질문은 아직 답을 찾지 못함

- 생성형 AI 모델이 직면한 법적 문제 증가는 기존 AI에 대한 법적, 윤리적 논쟁에 복잡성을 더하며, 아직 해결되지 않은 문제의 다양한 위험을 가중한다는 평가

▶ 데이터 스크래핑은 사용자의 개인정보보호권, 라이선스 및 오픈 소스 문제, 지식재산권 부문과 얽히면서 갈등이 고조되며, 최근 소송 제기가 빠르게 증가

- 이에 따라 전 세계 규제당국은 기존 법률을 통해 AI에 대한 규제를 강화하는 동시에 AI 관련 새로운 법체계 도입 논의가 시작됨
- 아직까지 각국 규제당국은 데이터 스크래핑을 개인정보보호 위협으로 직접 언급하지는 않고, 다양한 위험을 규정하고 이에 대한 대응을 요구하는 상황
- 데이터 스크래핑에 대한 규제 방향이 가장 혁신적인 기술로 평가되는 AI의 발전 방향을 크게 좌우할 것이라는 평가

#### Reference

1. Dataguidance, EU: Data scraping - navigating the challenges old and new, 2023.8
2. JD Supra, Data Scraping, Privacy Law, and the Latest Challenge to the Generative AI Business Model, 2023.7.18.
3. OAIC, Global expectations of social media platforms and other sites to safeguard against unlawful data scraping, 2023.8.24.
4. TechCrunch, Social media giants urged to tackle data-scraping privacy risks, 2023.8.25.

# EU 디지털서비스법(DSA)의 개인정보 보호 관련 규정 및 규제당국의 역할 분석

## [ 목 차 ]

1. EU 디지털서비스법(DSA) 개요
2. DSA의 개인정보보호 관련 주요 조항
  - (1) 맞춤형 광고 – 민감정보 및 아동 보호
  - (2) 다크패턴
  - (3) 연구자 및 관할 기관과의 정보 공유
  - (4) 불법 콘텐츠 제재
3. DSA 집행 프레임워크 및 집행기관의 역할
4. 요약 및 시사점

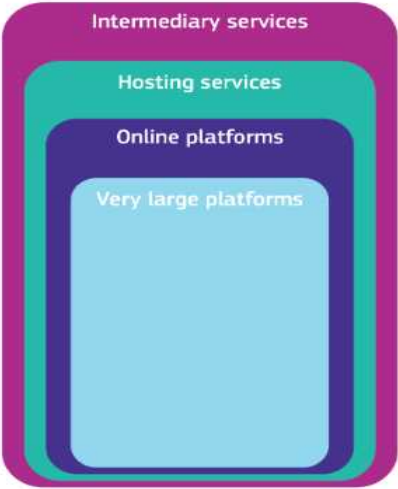
## 1. EU 디지털서비스법(DSA) 개요

- ▶ '20년 12월 EU 집행위원회가 제출하여 '22년 10월 제정된 디지털서비스법(Digital Services Act, DSA)은 EU 집행위원회의 '디지털 시대에 부합하는 유럽'<sup>2)</sup> 정책 의제 초석 중 하나로, 디지털시장법(Digital Market Act, DMA)과 함께 EU 내에서 온라인 플랫폼에 대한 규제를 강화하기 위해 마련
- 최근 EU는 포괄적인 디지털 규제 체계를 구축하고자 다양한 법률과 정책을 선보이고 있으며, 이러한 취지에서 제정된 DSA는 DMA와 더불어 일반 개인정보보호법(GDPR), 데이터 거버넌스법(Data Governance Act, DGA) 등과 상호 작용하는 관계를 형성

2) 'A Europe fit for the digital age'는 '19년~'24년 EU 집행위원회의 6대 주요 정책과제 중 하나로, EU 내 디지털 전환 및 디지털 규제 프레임워크의 확장을 목표로 함

- DSA는 캐싱 및 호스팅 서비스를 제공하는 중개 서비스 사업자를 포함하여 소비자를 상품, 서비스 및 콘텐츠에 연결하는 모든 디지털 서비스에 명확한 의무를 부과함으로써 ▲불법 콘텐츠 및 허위 정보 문제를 해결하고 ▲사용자에게 안전하고 투명한 온라인 환경을 조성하는 것을 목표로 함
- ▶ DSA는 디지털 서비스의 성격, 규모 및 영향력에 근거해 적용 대상을 크게 ▲중개 서비스 사업자 ▲호스팅 서비스 ▲온라인플랫폼 ▲대규모 온라인플랫폼 등의 단계로 분류하고, 권리와 의무는 나열 순서에 따라 누적 적용

그림 \_ DSA 적용 대상 단계 구분

	사업자 구분	설명
	중개 서비스	<ul style="list-style-type: none"> <li>• 네트워크 인프라 제공</li> <li>• 인터넷 액세스 제공업체, 도메인 이름 등록기관 및 아래의 호스팅서비스, 온라인플랫폼도 포함</li> </ul>
	호스팅 서비스	<ul style="list-style-type: none"> <li>• 클라우드 및 웹 호스팅 서비스와 같은 호스팅 서비스 및 아래의 온라인플랫폼도 포함</li> </ul>
	온라인플랫폼	<ul style="list-style-type: none"> <li>• 온라인 마켓플레이스, 앱 스토어, 협력 경제 플랫폼, 소셜 미디어 플랫폼 등 판매자와 소비자를 하나로 묶는 온라인 사업자</li> </ul>
	대규모 온라인플랫폼	<ul style="list-style-type: none"> <li>• 월간 사용자 수(MAU)가 4,500만 명(유럽 인구 4억 5,000만 명의 10%) 이상인 온라인플랫폼</li> <li>• 불법 콘텐츠를 유포하고 사회적 피해를 입힐 수 있는 특별한 위험 내포</li> </ul>

출처: European Commission<sup>3)</sup>

- DSA는 중개서비스 사업자를 ▲단순 전달 서비스 ▲캐싱 서비스 ▲호스팅 서비스 등을 제공하는 사업자로 구분

표 \_ DSA의 중개서비스 사업자 구분

구분	내용
단순 전달 서비스 (mere conduit service)	<ul style="list-style-type: none"> <li>• 통신망으로 정보를 전송하거나 통신망에 대한 접근을 제공하는 서비스</li> </ul>
캐싱 서비스 (caching service)	<ul style="list-style-type: none"> <li>• 정보를 효율적으로 전송하기 위한 목적으로 통신 네트워크를 통해 정보를 전송하는 것으로 구성된 서비스</li> </ul>
호스팅 서비스 (hosting service)	<ul style="list-style-type: none"> <li>• 서비스 이용자의 요청에 의해 제공된 정보의 저장으로 구성된 서비스</li> </ul>

3) [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en)



- 특히 DSA는 이러한 분류 체계를 기반으로 비례적인 의무를 부과하는 방식을 도입
  - 예컨대, 첫 번째 범주인 '중개서비스'에는 일반 의무사항만을 적용하며, 이보다 규모가 더 큰 사업자에게는 추가적으로 의무를 부과
  - EU 집행위원회는 '23년 4월, EU 전역 월간 사용자 수(MAU)가 4,500만 명 이상인 17개의 '초대형 온라인 플랫폼(VLOP)\*'과 2개의 '초대형 온라인 검색엔진(VLOSE)\*\*'을 지정했으며, DSA는 이러한 대규모 사업자들에게 가장 많은 책무를 부여<sup>4)</sup>

\* Very Large Online Platforms    \*\* Very Large Online Search Engine

표 \_ EU 집행위원회 지정 19개 VLOP 및 VLOSE

구분	서비스 종류	기업	디지털서비스
VLOP	소셜미디어	Google (Alphabet)	Youtube
		Meta	Facebook
		Meta	Instagram
		Bytedance	TikTok
		Microsoft	LinkedIn
		Snap	Snapchat
		Pinterest	Pinterest
		X (前 Twitter)	X
	앱 스토어	Google (Alphabet)	Google Play
		Apple	Apple App Store
	위키	Wikimedia	Wikipedia
	이커머스	Amazon*	Amazon Marketplace
		Google (Alphabet)	Google Shopping
		Alibaba Group	AliExpress
		Booking Holdings	Booking.com
		Zalando*	Zalando
	지도	Google (Alphabet)	Google Maps
VLOSE	검색 엔진	Google (Alphabet)	Google Search
		Microsoft	Bing

※ Amazon과 Zalando는 VLOP 지정에 불복하여 EU 사법재판소의 일반 법원에 소송을 제기한 상태

- 한편 GDPR과 마찬가지로 DSA 또한 역외 효력을 가지고 있어, 서비스 이용자가 EU에 소재하는 EU 시민일 경우, 서비스 사업자의 소재지가 EU 역내와 역외 관계없이 적용
- ▶ DSA 법률 자체는 EU 관보(Official Journal of the European Union)에 게재한 날('22.10.27.)로부터 20일 후('22.11.16) 효력이 발생했으나, 실질적인 운영을 위한 대부분 조항은 아래와 같이 '24년 2월 17일까지 점진적으로 적용될 전망<sup>5)</sup>

4) [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_23\\_2413](https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413)

표 \_ DSA 의무 적용 확대 타임라인

날짜	주요 내용	적용 대상
'23.2.17.	<ul style="list-style-type: none"> <li>투명성 보고 조치 이행 마감일(DSA 제24조제2항, 제3항)</li> </ul>	<ul style="list-style-type: none"> <li>모든 온라인 플랫폼 및 온라인 검색엔진 사업자</li> </ul>
'23.8.25.	<ul style="list-style-type: none"> <li>VLOP 및 VLOSE의 의무사항(DSA 제11조~제43조) 준수 마감일</li> </ul>	<ul style="list-style-type: none"> <li>VLOP 및 VLOSE</li> </ul>
'24.2.17.	<ul style="list-style-type: none"> <li>모든 중개 서비스 사업자에 적용되는 일반 의무사항(DSA 제11조~제15조) 준수 마감일</li> <li>특별 유형 서비스 사업자에 대한 추가적 의무 준수 마감일</li> <li>EU 회원국의 디지털 서비스 코디네이터(DSC) 지정 마감일</li> </ul>	<ul style="list-style-type: none"> <li>모든 중개 서비스 사업자</li> </ul>

- ▶ 이하 본 고는 DSA에서 명시하는 개인정보보호 관련 주요 의무사항을 소개하고 특히 DSA의 시행이 각국 규제기관 등에 미치는 영향을 고찰하고자 함

## 2. DSA의 개인정보 관련 주요 내용

### (1) 맞춤형 광고 – 민감정보 및 아동보호

- ▶ **(민감정보)** DSA 제26조제3항은 온라인 플랫폼 사업자가 '특수 범주의 개인정보'\*를 사용하여 GDPR에서 정의한 프로파일링\*\*을 기반으로 서비스 이용자에게 광고를 제공하는 행위를 금지

\* GDPR 제9조에서 언급하는 특수 범주의 개인정보를 뜻하며 인종, 민족, 정치, 종교, 노동조합 가입 유무, 유전자 정보, 생체정보, 건강정보, 성생활 정보, 성적 취향 정보를 포함하며 우리나라 개인정보보호법 제23조의 민감정보와 유사

\*\* 개인의 업무 성과, 경제적 상황, 건강, 개인적 선호, 관심사, 신뢰도, 행태, 위치 또는 이동 등 개인의 특정 측면을 평가하기 위해 개인정보를 사용하여 이루어지는 모든 형태의 자동화된 개인정보 처리를 지칭

- 동 금지 조항은 프로파일링 자체보다는 민감정보를 사용한 프로파일링을 기반으로 광고를 '제시'하는 행위와 관련이 있으나 GDPR에서 프로파일링을 기반으로 한 개인정보 처리에 대한 의무를 이미 규정하고 있으므로 DSA를 단독으로 해석·적용할 것이 아니라 GDPR과 함께 읽는 것이 필요

5) 일반적으로 EU 법령은 (1) 법령에서 특정 시행일을 정한 경우에는 해당 일자로부터 (2) 법령에서 별도로 규정하고 있지 않은 경우에는 공포일로부터 20일 경과한 날로부터 시행되나, 법령의 '시행일(date of entry into force)'과 '적용일(date of application)'이 반드시 일치할 필요는 없음. 특정 법령의 적용일은 공식 시행일 이후로 설정할 수 있으며, 만약 소급하여 적용할 만한 정당한 사유가 존재할 때에는 시행하는 날 이전으로 정할 수 있음. (European Union, Joint Practical Guide of the European Parliament, the Council and the Commission for persons involved in the drafting of European Union legislation, 2015, 68 페이지~71 페이지 참고)

- GDPR은 정보주체에게 프로파일링 및 프로필 정보에 기반한 맞춤형 광고에 대한 반대권과 자동화된 의사결정 대상이 되지 않을 권리를 보장하고 있음
- ▶ **(아동보호)** DSA 제28조는 “서비스 이용자가 미성년자임을 확신할 수 있는 경우”, 이용자의 개인정보를 사용하여 프로파일링에 기반한 광고를 인터페이스에 표시하는 것을 금지
- VLOP의 경우 매년 종합적인 위험 평가를 수행하여 자사 서비스가 아동의 권리에 미치는 부정적인 영향이나 사용자의 정신 및 신체에 미치는 영향을 측정해야 함
  - 특히 중독성 있는 행동으로 이어질 수 있는 알고리즘, 온라인 인터페이스 및 자동화된 의사결정 설계와 관련된 위험을 조사할 의무가 있음
  - 확인된 위험을 완화하기 위해 VLOP 사업자는 높은 수준의 개인정보보호, 보안 및 미성년자 안전을 보장할 수 있도록 시스템을 재설계하고 개인정보 처리 관행을 조정하는 등 적절한 조치를 취해야 함

## (2) 다크패턴

- DSA는 개인정보 처리 관련 동의 옵션을 시각적으로 두드러지게 표시하거나, 사용자에게 반복적으로 결정을 요청하거나 촉구하는 등 자유로운 선택을 왜곡하거나 저해할 수 있는 다크패턴을 포함한 사용자 기만적인 넛지(nudge) 기법을 금지(DSA 제25조)
  - 특히 DSA는 이와 같은 다크패턴 금지가 EU 집행위원회가 제정한 불공정상거래지침 (Unfair Commercial Practices Directive, UCPD) 또는 GDPR이 적용되는 관행에는 적용되지 않는다고 명시
  - 이와 관련하여 DSA는 EU 집행위원회가 다크패턴 금지가 특정 관행에 어떻게 적용되는지 안내하는 지침을 발행할 권한을 보유하고 있음을 강조
  - 한편 동 다크패턴 금지 조항은 온라인 플랫폼에게만 적용되는 의무사항임을 명시

## (3) 연구자 및 관할 기관과의 정보 공유

- ▶ DSA 제40조는 VLOP 및 VLOSE가 규정 준수 여부를 모니터링하는데 필요한 정보에 대한 접근 권한을 관할 당국에 제공해야 할 의무를 규정
- 관할 당국이란, EU 회원국에서 지정한 디지털 서비스 코디네이터(Digital Services Coordinator, DSC) 또는 EU 집행위원회를 지칭

- 이러한 접근 권한에는 합리적인 요청에 근거한 합리적인 기간 동안 알고리즘과 관련된 정보에 대한 접근 권한이 포함
- 또한 ▲조직적 위험의 탐지, 식별 및 이해에 기여하는 연구를 수행하기 위한 목적 ▲위험 완화 조치의 적절성, 효율성 및 영향 평가 목적으로 DSC의 요청에 의해 검증된 연구자에게 접근 권한을 제공할 의무를 제시하고 있음
- 한편, 이와 같이 플랫폼 데이터에 대한 접근을 제공하는 것은 많은 경우 개인정보에 대한 접근을 제공하는 것을 수반하며, 이와 같은 개인정보 처리는 GDPR의 적용 범위에 포함되기에 컨트롤러의 의무를 유발
  - DSA 전문 제98조는 사업자 및 연구자 모두 GDPR에서 규정한 개인정보 처리 관련 정보주체의 권리 보호 의무 준수에 특히 주의를 기울여야 한다는 점을 강조

#### (4) 불법 콘텐츠 제재

- ▶ DSA 제16조는 온라인 플랫폼을 포함한 호스팅 서비스가 불법 콘텐츠를 삭제할 의무를 명시하고 있으며, 이는 개인 또는 기관의 신고를 통한 통지 및 조치 메커니즘(notice-and-action mechanism)을 기반으로 함
- 호스팅 서비스는 “충분히 정확하고 적절하게 입증된 통지”를 쉽게 제공할 수 있는 메커니즘을 마련할 의무를 강조
  - 한편, GDPR이 컨트롤러에게 삭제 요청을 포함한 정보주체의 권리 행사를 용이하게 “부당한 지체 없이” 요청을 받은 시점으로부터 1개월 이내 취한 조치에 대한 정보를 전달할 것을 요구하는 데 반해, DSA는 불법 콘텐츠 삭제에 대한 통지를 처리하는 구체적인 일정을 제시하고 있지 않음
- VLOP 및 VLOSE의 경우 특정 유형의 불법 콘텐츠와 관련된 통지의 처리 속도와 품질, 신속한 삭제 등 콘텐츠 조정 프로세스의 채택을 보장하는 완화 조치를 통지 및 조치 메커니즘에 추가로 설계해야 함

표 \_ 적용 대상에 따른 누적 의무사항

의무사항	중개서비스	호스팅 서비스	온라인 플랫폼	VLOP
투명성 보고	○	○	○	○
기본권 관련 조건	○	○	○	○
국가 당국과의 협력	○	○	○	○

의무사항	중개서비스	호스팅 서비스	온라인 플랫폼	VLOP
연락 창구 및 법정 대리인	○	○	○	○
사용자에 대한 통지 및 조치 의무		○	○	○
형사 범죄 신고		○	○	○
민원·구제 메커니즘 및 법정 외 분쟁 해결			○	○
신뢰할 수 있는 신고자			○	○
허위 신고 및 이의제기 신고에 대한 조치			○	○
Marketplace에 대한 특별 의무			○	○
아동 대상 맞춤형 광고 및 사용자의 특수성에 기반한 광고 금지			○	○
추천 시스템의 투명성			○	○
온라인 광고의 투명성			○	○
위험 관리 및 위기 대응 의무				○
외부 독립적인 감사, 내부 컴플라이언스 및 공적 책임				○
프로파일링에 기반한 추천을 받지 않을 사용자 선택권				○
연구자 및 관할 기관과의 정보 공유				○
행동 강령				○
위기 대응 조정				○

출처: PwC<sup>6)</sup>, 넥스텔리전스(주) 재구성

### 3. DSA 집행 프레임워크 및 집행기관의 역할

▶ **(개요)** DSA의 이행을 위해 각국 규제당국과 EU 집행위원회 사이에 EU 차원의 협력 메커니즘 구축

- EU 집행위원회는 VLOP 및 VLOSE에 대한 주요 집행기관으로, 해당 기업들을 모니터링하고 제재할 수 있는 권한을 보유

6) <https://www.pwc.nl/en/insights-and-publications/themes/digitalization/thorough-revision-of-the-rules-for-online-platforms.html>

- 이처럼 중앙 집중화된 집행 방식은 다수 국가가 연관된 사건에 있어 각국 개인정보 감독기관(DPA)과 EU 개인정보보호 이사회(EDPB)를 통한 일명 '원스톱숍 메커니즘'을 통해 집행을 보장하는 GDPR과는 대조
- VLOP 및 VLOSE가 아닌 기타 사업자들에 대한 집행은 각국 DSC를 따름
- ▶ **(EU 회원국)** EU 회원국은 '24년 2월 17일까지 DSC를 지정하여 자국 영토에 설립된 서비스가 DSA를 준수하는지 감독하고, DSA법에서 규정한 EU 협력 메커니즘에 참여해야 함
- DSC는 공정하고 투명하게 업무를 수행해야 하는 강력한 요건을 갖춘 독립적인 기관이 될 것이며, EU 역내에서 DSA 집행의 일관성과 디지털 역량을 보장하는 역할을 수행하기 위해 '유럽 디지털 서비스 코디네이터(European Board for Digital Services)'라는 독립 자문 그룹과 협력
  - 각국 DSC는 유럽 디지털 서비스 코디네이터와 협력하여 분석, 보고서 및 권고 사항을 지원하고 새로운 공동 조사 장치를 마련하는데 지원할 계획
  - 또한 DSC는 DSA가 서비스 사용자에게 부여한 권리 행사와 관련한 민원에 대한 대응을 담당
- EU 회원국은 DSA 위반에 대해 자국에서 부과할 수 있는 과징금에 대한 규칙을 채택해야 함
- ▶ **(EU 집행위원회)** EU 집행위원회는 현행 반독점 규정에 따른 감독 권한과 동일하게 조사 권한과 전 세계 매출의 최대 6%에 달하는 과징금을 부과할 수 있는 권한을 가짐
- 또한 EU 집행위원회는 온라인 플랫폼에 위반 사항을 시정하기 위해 필요한 조치를 취하도록 요청할 수 있으며, 서비스 사용자에게 심각한 피해가 발생할 위험이 있는 긴급한 경우, 해당 침해에 대한 조사가 완료되기 전에 임시 조치를 명령할 권한이 있음
- ▶ **(ECAT)** 유럽 알고리즘 투명성 센터(European Centre for Algorithmic Transparency, ECAT)는 위험 관리 및 완화 의무 관련 VLOP 및 VLOSE에 대해 평가함에 있어 EU 집행위원회를 지원
- ECAT은 공정성, 책임성 및 투명성을 평가하기 위해 원칙에 기반한 접근 방식을 채택

#### 4. 결론 및 시사점

- ▶ DSA의 다수 의무사항은 GDPR에서 이미 규정하고 있는 의무와 밀접한 관련성이 있는 만큼, GDPR과의 일관성을 위해 EU 집행위원회를 비롯해 DSA 집행기관과 GDPR 집행기관 간의 긴밀한 협력이 필요
- DSA와 GDPR 체계 간의 상호 작용이 두드러짐에도 불구하고 현 DSA 집행 프레임워크는 DPA, EDPB, 또는 EDPS와의 협력 및 조정을 별도 언급하고 있지 않으므로, 협력 및 조정 프로세스를 설정하기 위한 노력이 필요할 것으로 예상
- ▶ 또한 DSA에서 향후 다른 규정들과의 일관적인 법 해석과 적용을 위한 지침 마련을 예고한 바 있으므로, DSA의 적용 단계에서 EU 집행위원회와 기타 감독기관 간 논의가 본격화될 것으로 전망

#### Reference

1. 5Rights Foundation, EU Digital Services Act comes into effect, requiring a high level of privacy, safety and security for children, 2022.11.
2. DSA Observatory, The Digital Services Act: Adoption, Entry into Force and Application Dates, 2022.9.12.
3. EUR-Lex, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), 2022.10.27.
4. European Commission, Questions and Answers: Digital Services Act, 2023.4.25.
5. Future of Privacy Forum, EU's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay with the GDPR, 2023.8.31.



〈2023년 개인정보보호 월간 동향 보고서 발간 목록〉

번호	호수	제 목
1	1월 01	주요국 개인정보보호 강화기술 정책동향 분석 및 시사점
2	1월 02	EU 인공지능법(안)과 GDPR의 상호작용 분석
3	1월 03	해외 아동 개인정보 보호 침해 관련 행정처분 사례 분석
4	2월 01	해외 경쟁법 관련 개인정보보호 이슈 분석
5	2월 02	미국의 개인정보보호 법제 입법 동향
6	2월 03	디지털 자산과 개인정보보호의 관련성 및 고려사항
7	3월 01	웹 3.0 시대 도래로 부상하는 개인정보보호 이슈 분석
8	3월 02	사우디아라비아의 데이터·프라이버시 규제 샌드박스 추진현황
9	3월 03	개인정보보호와 활용성 강화 기술로 주목받는 재현데이터 기술의 특성과 활용 과제
10	4월 01	2023년 주요 개인정보보호 실태 서베이 보고서 분석
11	4월 02	ChatGPT의 등장과 주요국의 개인정보보호 규제 동향
12	4월 03	2022년 4분기 EDPB 총회 주요 결과 분석
13	5월 01	해외 주요 개인정보 감독기관 연례보고서 주요 내용 및 활동성과
14	5월 02	EDPS 2022 연간 활동 보고서 분석
15	5월 03	안면인식기술 제재 관련 정책 추진 및 분석과 평가
16	6월 01	2023년 상반기 개인정보 규제 위반에 대한 해외 주요국 제재 및 처분 사례 분석
17	6월 02	EDPB의 개인정보 역외 이전 지침 주요 내용 분석
18	6월 03	영국 개인정보 감독기관(ICO)의 DSAR 기업 대응 지침 분석 및 평가
19	7월 01	미국의 소비자 건강·의료 개인정보 침해 사례와 입법 동향 분석
20	7월 02	국내외 정보주체 삭제권(잊힐 권리) 강화 동향
21	7월 03	CCTV 설치·운영에 관한 최근 개인정보보호 주요 지침과 이슈 분석
22	8월 01	EU 집행위원회의 웹 4.0 및 가상세계 전략으로 본 EU의 메타버스 개인정보 보호 이슈 및 대응 동향
23	8월 02	Apple · Google의 서드파티 쿠키 퇴출 정책 현황 분석
24	8월 03	EU-미국 데이터 프라이버시 프레임워크[DPF] 주요 내용 및 시사점

25	9월 01	미국 데이터브로커 관련 규제 및 정책 동향
26	9월 02	데이터 스크래핑에 대한 12개 개인정보 감독기관의 공동 성명 발표와 관련 주요 이슈
27	9월 03	유럽 DSA와 개인정보보호 규제당국의 주요 역할 분석

# 2023

## 개인정보보호 월간동향분석 제9호

**발행** 2023년 10월 5일

**발행처** 한국인터넷진흥원  
개인정보본부 개인정보정책팀  
전라남도 나주시 진흥길 9  
Tel: 061-820-1865

1. 본 보고서는 개인정보보호위원회 「개인정보보호 동향 분석」 사업 수행 결과물입니다.
2. 본 보고서의 저작권은 한국인터넷진흥원에 있으며, 본 보고서를 활용하실 경우에는 출처를 반드시 밝혀주시기 바랍니다.
3. 본 보고서의 내용은 한국인터넷진흥원의 공식 입장과는 다를 수 있습니다.