2021 Privacy Report

개인정보보호 월간동향분석

제 9 호

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2021 Privacy Report

개인정보보호 월간동향분석

제 9 호

1. 중국 개인정보보호법 제정과 시사점

2. 네덜란드의 틱톡 규제를 통해 본 아동 개인정보보호 위반 사례 분석

3. EU의회 싱크탱크의 산업데이터 공유 관련 보고서 분석

KISA

중국 개인정보보호법 제정과 시사점

[목 차]

1. 개요

- 중국 개인정보보호법 최종 법안이 2021년 8월 20일 통과되어 2021년 11월 1일부터 시행 예정
- 중국은 이전까지 다양한 법률을 통하여 개인정보를 보호해 왔으나 동 법률 제정으로 개인정보보호 관련 일반법 체계를 구축

2. 중국 개인정보보호법의 주요 내용

(1) (구성) 8장 74조로 구성

(2) (주요 내용) 적용 대상과 개인정보 처리 원칙, 개인정보 국외 이전, 개인의 권리, 개인정보 처리자의 의무, 개인정보 보호 담당 부처와 권한, 위반 시 처벌 등을 규정

(3) (초안과 최종 법안의 주요 차이) 자동화 의사결정을 이용한 가격차별 정책의 명시적 금지, 만 14세 미만 아동에 대한 민감 개인정보 지정, 중요 인터넷 플랫폼 서비스의 개인정보 보호 의무 강화 등

3. 시사점

최종 승인된 중국 개인정보보호법은 인터넷 플랫폼 사업자에 대한 규제를 강화한 것이 특징으로 빅테크 기업 타격이 예상되며, 유럽의 GDPR과 유사한 수준의 강력한 규제를 담고 있어 법 적용을 받는 우리 기업의 사전 대비가 필요

1. 개요

▶ 중국 전국인민대표대회는 '20년 10월 처음 개인정보보호법 초안을 발표한 이후 2차례의 의견수렴을 거쳐 수정된 법안을 '21년 8월 20일 최종 승인하고 11월 1일부터 시행 예고

- 개인정보보호법이 통과되기 전까지 중국은 네트워크안전법, 형법 등 다양한 법률을 통해 개인정보를 보호해 왔음
- 그러나 디지털 경제의 발전과 함께 개인정보의 수집과 이용이 급증하여 개인정보 보호에 관한 내용을 통합적으로 다루는 전문 법령의 필요성이 대두되면서 개인정보 보호법이 제정되기에 이르렀음

▶ 최종 승인된 법률은 '20년 10월 발표된 초안의 내용을 대부분 유지하고 있으나 초안 발표 이후 2차례의 의견 수렴을 통해 유의미한 수준의 조항 수정과 추가가 이루어짐

- 일례로 대규모 이용자를 보유한 주요 인터넷 플랫폼 서비스에 대한 개인정보 보호 요구사항이 추가되었으며 자동화된 의사결정을 이용한 가격 차별정책을 명시적으로 금지함

2. 중국 개인정보보호법의 주요 내용

(1) 구성

- 중국 개인정보보호법은 전체 8장, 74개 조항으로 구성

표1 _ 중국 개인정보보호법의 구성

장·절	조
제1장 총칙	제1조 목적[1]
	제2조 개인정보의 중요성
	제3조 적용 대상
	제4조 개인정보 및 개인정보 처리
	제5조 개인정보 처리 방식
	제6조 개인정보 처리 목적
	제7조 개인정보 처리 원칙
	제8조 개인정보 정확성
	제9조 개인정보 보안
	제10조 개인정보 처리 시 법률 준수
	제11조 개인정보 보호 제도 수립 등
	제12조 개인정보 보호 분야 국제 교류 등

장·절		조
제2장 개인정보 처리 규칙	제1절 일반 규정	제13조 개인정보 처리 조건
		제14조 개인정보 처리 동의
		제15조 동의 철회 권리
		제16조 부동의 또는 동의 철회 시 상품, 서비스 제공
		제17조 개인정보처리자 관련 정보 고지
		제18조 고지 면제, 사후 고지
		제19조 개인정보 보관 기간
		제20조 복수의 개인정보처리자
		제21조 개인정보 처리 위탁
		제22조 합병, 분할에 따른 개인정보 이전
		제23조 개인정보 제3자 제공
		제24조 개인정보를 이용한 자동 의사 결정
		제25조 개인정보 공개 금지
		제26조 이미지 수집, 개인신분 식별 설비 설치
		제27조 공개된 개인정보 처리
	제2절 민감 개인정보 처리 규칙	제28조 민감 개인정보 처리 목적 및 필요성
		제29조 민감 개인정보 처리 시 개인 동의
		제30조 개인에게 처리 필요성 및 영향 고지
		제31조 14세 미만 미성년자 개인정보 처리 시 보호자 동의
		제32조 관련 법률, 행정법규 준수
	제3절 국가기관의 개인정보 처리 특별 규정	제33조 국가기관의 개인정보 처리 행위에 대한 법률 적용
		제34조 개인정보 처리 시 법률 준수
		제35조 개인에게 고지 및 동의
		제36조 개인정보 증국 내 보관
		제37조 국가기관의 개인정보 취급에 관한 규정
제3장 개인정보 국외 이전 규칙		제38조 개인정보 국외 제공 조건
		제39조 개인에게 고지 및 동의
		제40조 주요정보기반시설 운영자 등의 개인정보 국내 보관
		제41조 사법 공조 등을 위한 개인정보 국외 제공
		제42조 개인정보 제공 제한 또는 금지 목록
		제43조 국가, 지역에 상응하는 조치(상호주의)
제4장 개인정보 처리 행위에 관한 개인의 권리		제44조 개인정보 처리에 대해 알 권리 및 결정권
		제45조 개인정보 열람, 복제 요구권
		제46조 개인정보 정정, 보완 요구권
		제47조 개인정보처리자의 개인정보 파기
		제48조 개인정보 처리 규칙에 대한 해석, 설명 요구권
		제49조 고인의 개인정보에 대한 열람, 복제, 수정, 삭제권
		제50조 개인의 권리 행사를 위한 프로세스 수립
제5장 개인정보처리자의 의무		제51조 개인정보 보호 조치
		제52조 개인정보 보호 책임자 지정
		제53조 국외 개인정보처리자의 중국 내 전문기관 설립 혹은 대표자 지정
		제54조 정기적 심사

장·절	조
	제55조 사전 개인정보보호 영향평가의 실시
	제56조 개인정보보호 영향평가의 내용
	제57조 개인정보 구제 조치 및 유출 통지
	제58조 중요 인터넷 플랫폼 서비스 제공자의 의무
	제59조 개인정보 처리 수탁자의 의무
제6장 개인정보 보호 직무 담당 부처	제60조 개인정보 보호 직무 담당 부처
	제61조 개인정보 보호 업무
	제62조 개인정보 보호 관련 규칙, 표준 제정
	제63조 개인정보 보호 업무 관련 조치
	제64조 개인정보처리자와 회의(면담)
	제65조 기관, 개인의 민원 제기 및 신고 권리
제7장 법률적 책임	제66조 법률 위반 시 벌금 부과
	제67조 위법 행위 기록 및 공시
	제68조 국가기관에 대한 처벌
	제69조 개인정보 권익 침해에 대한 배상
	제70조 다수 개인의 권익 침해 시, 소송 제기
	제71조 법률 위반 시 형사 처벌
제8장 부칙	제72조 적용 예외
	제73조 용어 정의
	제74조 시행일

(2) 주요 내용

▶ 중국 개인정보보호법은 적용 대상과 개인정보 처리 원칙, 개인정보 국외 이전, 개인의 권리, 개인정보처리자의 의무, 개인정보 보호 담당 부처와 권한, 위반 시 처벌 등을 규정

- **(법의 적용 대상)** 중국 내에서 개인정보를 처리하는 경우뿐만 아니라 중국 외에서 중국인의 개인정보를 처리하고 특정 기준*에 해당하는 경우에도 적용이 가능함(제3조)

* 제3조 (1) 국내 자연인에게 상품 또는 서비스를 제공하는 목적, (2) 국내 자연인의 행위를 분석, 평가, (3) 법률 및 행정법규 상 규정된 기타 사항

- **(개인정보 처리 원칙)** 개인정보 처리 시 합법적이고 정당한 방식, 명확하고 합리적인 목적, 처리 목적과 부합하는 처리, 공개적이고 투명한 원칙 준수, 개인정보 처리 규칙 명시 등이 필요하다고 규정(제5조~제7조)

  - 개인정보 처리는 개인 동의뿐만 아니라, 계약 체결·이행, 법적 의무 이행, 위급 상황, 공공의 이익, 타 법률 규정 등에 해당되는 경우 가능(제13조)

  - 개인정보 처리 전 개인정보처리자의 연락처, 개인정보 처리 목적·방식·유형, 보관기간, 개인 권리 행사 방식·절차, 기타 사항 등을 개인에게 고지(제17조)

1) 중국어 원문에는 조항 제목이 없으며, 이해를 돕기 위해서 작성하였음

- 복수의 개인정보처리자가 개인정보 처리 목적·방식을 결정 시, 각자 권리와 의무를 정하며, 개인 권익 침해 시 연대 책임(제20조)

- 개인정보처리자의 수탁자 감독, 합병·분할로 인한 개인정보 이전, 개인정보 제3자 제공(제21조~제23조)

- 개인정보를 이용한 자동 의사 결정 시 개인의 설명 요구 및 거절 권리 보장(제24조)

- 공공장소에서 이미지 수집, 개인정보 식별 설비 설치 시 공공안전보호를 위한 목적으로만 가능(제26조)

- 민감 개인정보* 처리 시, 개인으로부터 별도 동의를 받아야 하며, 처리 필요성, 개인에게 미치는 영향을 고지하고 14세 미만 미성년자 개인정보 처리 시 부모 또는 기타 보호자 동의 필요(제28조~제30조)

  * 제28조: 민감 개인정보란 일단 유출되거나 불법적으로 사용되면 개인의 인격 존엄성을 해치거나 신변, 재산 안전상 피해를 입을 수 있는 정보로, 생물학적 특징, 종교신앙, 특정 신분, 의료건강, 금융 계좌, 개인 행적 등의 정보 및 14세 미만 미성년자의 개인정보를 의미

• **(개인정보 국외 이전)** 개인정보 국외 이전 시 조건* 충족, 개인에게 관련 정보** 고지 및 별도 동의(제38조~제39조)

* 제38조: (1) 본 법률 제40조 규정에 근거하여 국가 네트워크 정보 부처 기관의 안전성 평가 통과, (2) 국가 네트워크 정보 부처 규정에 근거하여 전문 기관의 개인정보 보호 인증 진행, (3) 국외에서 개인정보를 이전받는 자와 계약을 체결하여 양측의 권리와 의무를 약정하고 개인정보 처리 행위가 본 법률에서 규정하는 개인정보 보호 표준에 부합하는지를 감독, (4) 법률, 행정 법규 또는 국가 네트워크 정보 부처에서 규정한 기타 조건

** 제39조: 해외에서 정보를 이전받는 자의 신분, 연락처, 처리 목적, 처리 방식, 개인정보 유형, 정보를 이전받는 해외 주체에게 본 법률에 규정된 권리를 행사하는 방법 등

- 주요정보기반시설 운영자*와 개인정보 처리 규모가 국가 네트워크 정보 부처가 정한 특정 기준에 해당하는 개인정보처리자의 개인정보 중국 내 보관, 국외 이전 시 안전성 평가 통과(제40조)

* 네트워크안전법 제31조: 주요정보기반시설은 공공통신, 정보서비스, 에너지, 교통, 수리, 금융, 공공서비스, 전자정무 등 중요 산업과 영역에서 파괴, 기능 상실, 데이터 유출이 발생하면 국가 안전, 국가 경제, 국민 생활 공공이익에 중대한 손실을 줄 수 있는 시설

- 국제 사법 공조 또는 행정 상 협조를 위하여 개인정보 국외 이전 시 주관 부처의 승인(批准)(제41조)

- 국외 기관·개인이 중국 국민의 개인정보 권익 침해, 중국의 국가 안보, 공공이익 위협 시, 개인정보 제공 제한·금지 목록*에 포함하고 개인정보 제공 제한·금지 조치(제42조)

* 일종의 블랙리스트(blacklist)로 중국 정부에서 해외 서비스를 차단하는 근거 조항으로 활용 가능

- 임의 국가·지역이 중국에 차별적 금지, 제한 시 해당 국가·지역에 상응하는 조치 가능(제43조)

- **(개인의 권리)** 개인의 개인정보 처리 관련 알 권리, 개인정보 처리 결정·제한·거절 권리, 개인정보 열람·복제·전송·정정·보완·파기·해석·설명 요구 권리, 고인의 개인정보에 대한 열람·복제·정정·파기 권리(제44조~제49조)

- **(개인정보처리자의 의무)** 개인정보처리자의 개인정보 보호 조치 수행, 개인정보 보호 책임자 지정, 정기적 심사, 사전 위험 평가, 개인정보 유출 시 구제 조치 및 통지(제51조~제52조, 제54조~제57조)

  - 국외 개인정보처리자의 경우 중국 내 전문 기관 설립 혹은 대표자 지정, 개인정보 보호 직무 담당 부처에 보고(제53조)

  - 중요 인터넷 플랫폼 서비스 제공자의 경우 독립 외부 감독기구 설치, 법령 위반한 제품과 서비스 기업에 대한 서비스 제공 중단, 개인정보 보호 관련 사회적 책임 보고서 발간(제58조)

- **(개인정보 보호 담당 부처 및 권한)** 국가 네트워크 정보 부처*가 개인정보 보호 및 관련 감독과 관리를 총괄하고 국무원 유관부처는 동 법과 관련 법률 및 행정규정에 의거해 각자의 책임 영역 내에서 개인정보 보호와 및 감독 관리를 수행(제60조)

  * 국가인터넷정보판공실을 지칭

  - 개인정보 보호 담당 부처는 개인정보 보호 홍보·교육, 불만·신고 접수 처리, 앱에 대한 개인정보 보호 현황 평가, 불법행위 조사 등을 수행(제61조)

  - 개인정보 보호 담당 부처는 개인정보 보호 업무 수행 시 관계자 조사, 관계자 계약, 기록 등 관련 자료 열람과 복사, 불법 활동이 의심되는 현장 조사 등의 실시 가능(제63조)

  - 개인정보 보호 담당 부처가 개인정보 처리활동에서 비교적 큰 위험 또는 개인정보 보안사고 발생 사실을 발견한 경우 개인정보처리자의 법정대리인이나 주책임자를 소환하거나 전문기관에 준법감사를 요구 가능(제64조)

- **(위반 시 처벌)** 법률의 심각한 위반 시 최대 5,000만 위안(약 90억 원) 이하 또는 전년도 매출액의 5% 이하의 벌금형, 소득 몰수, 업무 정지, 영업 중단, 영업 허가 취소 등 처벌* 가능(제66조)

  * 제66조: (1) 법률 위반으로 담당 부처의 시정 명령을 받았으나 미 시정 시, 100만 위안 이하 벌금 부과. 직접적인 책임을 지는 주요 관리자와 담당자는 1만 위안 이상 최대 10만 위안 이하의 벌금 부과. (2) 심각한 위반인 경우, 시정 명령, 위법하게 발생한 소득 몰수, 5000만 위안 이하 또는 전년도 매출액의 5% 이하 벌금 부과. 추가적으로 관련 업무 정지, 영업 중단, 영업 허가 취소 명령 가능. 직접적인 책임을 지는 주요 관리자와 담당자는 10만 위안 이상 최대 100만 위안 이하의 벌금 부과.

  - 국가기관의 개인정보 보호 의무 미 이행 시, 시정 명령 및 책임자 처분(제68조)

- 개인정보 권익 침해 시, 개인의 손실 혹은 개인정보처리자의 수익에 근거하여 배상(제69조)

- 다수의 권익 침해 시, 담당 기관이 인민법원에 소송 제기(제70조)

• **(용어 정의)** 개인정보처리자, 자동 의사 결정, 비식별화, 익명화 용어 정의*(제74조)

* 제69조: (1) 개인정보처리자란 자체적으로 처리 목적, 처리 방식 등 개인정보 처리사항을 결정하는 기관, 개인 (2) 자동 의사 결정이란 개인정보를 이용하여 개인의 행위 습관, 관심사 또는 경제, 건강, 신용정보 등을 컴퓨터 프로그램으로 자동 분석, 평가하고 의사를 결정하는 행위 (3) 비식별화란 개인정보를 처리하여 추가 정보의 도움 없이는 특정 자연인을 식별하지 못하도록 만드는 과정 (4) 익명화란 개인정보를 처리하여 특정 자연인을 식별하지 못하게 하며 다시 복원하지 못하도록 만드는 과정

(3) 초안과 최종 법안의 주요 차이

▶ 자동화 의사결정을 이용한 가격차별 정책의 명시적 금지(제24조)

• 개인정보처리자가 자동화 의사결정 방식으로 개인정보를 이용할 경우, 해당 결정의 투명성과 결과의 공평성·공정성을 보장해야 하며, 거래가격 등 거래조건에서 개인에게 비합리적인 차별대우를 할 수 없음

▶ 만 14세 미만 아동의 개인정보를 민감 개인정보에 포함(제28조)

• 개인정보보호법 제1차와 제2차 초안은 만 14세 미만 아동의 개인정보 수집 시 부모나 기타 보호자의 동의를 요구했으나 최종 법안은 한 발 더 나아가 14세 미만 아동의 개인정보를 민감 개인정보에 포함시킴

• 이에 따라 개인정보처리자는 특별한 목적과 필요성이 있으며 엄격한 보호조치가 취해진 경우에만 아동 개인정보를 처리 가능

• 만 14세 미만 아동의 개인정보를 처리하는 개인정보처리자는 아동 개인정보 처리를 위한 전문 개인정보처리규칙을 제정해야 함

▶ 외국 정부기관에 대한 개인정보 제공 제한 규정의 신설(제41조)

• 중국 개인정보보호법의 적용을 받는 개인정보처리자는 중국 정부의 승인 없이 중국 본토에 보관된 개인정보를 외국 정부에 제공할 수 없음

▶ 개인의 개인정보 이전권 신설(제45조)

• 최종 법문은 제45조에서 개인이 자신이 지정한 개인정보처리자에게 개인정보를 이전하도록 요구할 경우, 국가 네트워크 정보 부처의 규정과 조건에 부합된다면 개인정보처리자는 해당 개인에게 정보를 이전할 방법을 마련해주어야 한다고 규정

▶ 고인의 개인정보 사용권 규정 보완(제49조)

- 개인정보보호법 제2차 초안은 고인의 개인정보 관련 권리를 법에서 규정한 가까운 친족이 행사한다고 규정

- 최종 법문은 가까운 친척이 고인의 의사에 반하여 정보를 사용할 가능성을 방지하기 위해 고인이 생전에 별도로 정한 경우를 제외하고 적법하고 정당한 이득 취득을 위해 열람·복제·수정·삭제 관련 권리에 한하여 행사할 수 있도록 수정됨

▶ 중요 인터넷 플랫폼 서비스의 개인정보 보호 의무 강화(제58조)

- 최종 법문은 대규모 사용자를 보유하고 사업모델이 복잡한 중요 인터넷 플랫폼 서비스를 제공하는 개인정보처리자는 다음과 같은 의무를 이행해야 한다고 규정

  - 국가규정에 따라 개인정보 보호 준법제도를 수립하고 개인정보 보호 현황을 감독하기 위해 외부 인사로 구성된 독립 기구를 설치

  - 투명·공평·공정의 원칙을 견지하고 플랫폼 규칙을 제정하여 플랫폼 내 제품이나 서비스 제공자의 개인정보 처리 규칙과 개인정보 보호 의무를 명확히 함

  - 개인정보 처리 시 법률과 행정법규를 심각하게 위반한 제품이나 서비스 제공자에 대한 서비스 제공 중단

  - 개인정보 보호에 대한 사회적 책임 보고서를 정기적으로 발간하여 사회의 감독을 받음

▶ 개인정보보호법 총괄 규제기관의 지정 및 역할 규정(제62조)

- 제1차 초안은 국가 네트워크 정보 부처와 국무원 유관부처를 개인정보 보호 직무 담당 부처로 정하고, 각자의 책임 영역 내에서 개인정보 보호 업무를 추진하도록 규정

- 최종 법문은 국가 네트워크 정보 부처가 단독으로 유관부처와 조율을 거쳐 다음과 같은 개인정보 보호 업무를 진행하도록 역할을 명문화

  - 개인정보 보호를 위한 세부 규칙과 표준의 제정

  - 소규모 개인정보처리자, 민감 인인정보의 처리와 얼굴인식, 인공지능 등 신기술과 신규 응용서비스 대상 전문 개인정보 보호규칙과 표준의 제정

  - 안전하고 편리한 전자신원인증 기술의 연구개발과 보급의 지원 및 온라인 신원인증 공공서비스의 구축 촉진

  - 개인정보 보호를 위한 사회 서비스 체계 수립을 추진하고 관련 기관의 개인정보 보호 평가와 인증 서비스 지원

  - 개인정보 보호 관련 불만 신고 체계의 완비

3. 시사점

▶ '21년 8월 20일 최종 승인된 중국 개인정보보호법은 작년 10월 발표된 초안과 비교해 중국 국내외의 입법 동향과 산업 트렌드를 반영해 유의미한 수정이 이루어졌으며, 인터넷 플랫폼 사업자에 대한 규제를 강화한 것이 특징

- 자동화 의사결정을 이용한 가격차별 정책의 금지는 지난 해 중국 인터넷 플랫폼들이 자사 서비스만 이용하는 소비자에게 빅데이터와 알고리즘을 이용해 더 높은 가격을 책정한 행위가 논란이 되면서 새롭게 추가된 조항

- 중요 인터넷 플랫폼 사업자의 강화된 개인정보 보호 의무는 미국 및 유럽 정부의 빅테크 규제 흐름*을 반영한 것으로, 데이터 수집과 활용에 제한을 받는 빅테크 기업의 타격이 불가피할 전망

※ 미국 바이든 대통령은 2021년 7월 9일 빅테크 기업을 겨냥해 경쟁 촉진과 독점적 관행 단속을 지시하는 행정명령에 서명했으며, 유럽연합은 '20년 디지털시장법(Digital Market Act) 초안을 발표하며 시장 지배적 지위를 보유한 '게이트키퍼' 사업자 규제를 추진

▶ 월스트리트저널 등 해외 언론은 이번 개인정보보호법에 대해 유럽 GDPR과 유사하게 세계에서 가장 강력한 수준이라고 평가했으며, 위반 시 처벌은 EU GDPR보다도 엄격한 기준이 될 수 있다*고 보도

※ GDPR은 위반 시 최대 과징금은 2,000만 유로(약 270억 원) 또는 전 세계 매출액의 4% 중 큰 쪽을 적용하나 중국개인정보보호법은 위반 시 벌금은 최대 5,000만 위안(약 90억 원) 이하 또는 전년도 매출액의 5% 이하에 달하며 추가적으로 소득 몰수, 업무 정지, 영업 중단, 영업 허가 취소 등 처벌 가능

▶ 중국 개인정보보호법은 최상위 법으로서 구체적인 법 적용은 법률 담당 부처인 국가인터넷판공실이 발간할 세부 규정과 가이드라인에 의해 이루어질 전망으로, 법 적용을 받는 기업들은 지속적 관심을 기울일 필요가 있음

- 동 법은 중국 역내에 위치한 기업뿐 아니라 해외에서 중국 시민의 개인정보를 처리하는 경우에도 적용되는 만큼, 중국을 대상으로 사업을 영위하는 우리 기업들의 대비 필요

- 특히 주요정보기반시설에 해당하거나 처리하는 개인정보의 수가 많은 기업들은 개인정보 국외이전 시 안전성 평가를 거쳐야 하므로 사전 준비가 요구됨

Reference

1. 中国人大网, "中华人民共和国个人信息保护法", 2021.8.20.
2. China Briefing, "China's Personal Information Protection Law: A Comparison of the First Draft, the Second Draft, and the Final Document", 2021.8.24.
3. Stanford, "Seven Major Changes in China's Finalized Personal Information Protection Law", 2021.8.23.
4. The Diplomat, "China's Personal Information Protection Law and Its Global Impact", 2021.8.31
4. 법률신문, "중국 개인정보보호법 출범, 유럽보다는 유연하게 미국보다는 엄격하게", 2021.8.26

네덜란드의 틱톡 규제를 통해 본 아동 개인정보보호 위반 사례 분석

[목 차]

1. 개요

(1) 네덜란드 내 미성년자층을 중심으로 한 틱톡 서비스 성장

(2) 네덜란드 내 틱톡 서비스의 개인정보 제재 현황 요약

2. 틱톡의 아동 개인정보보호 위반 소송 및 과징금 사례

(1) 시장정보연구재단(SOMI)

(2) 네덜란드소비자연합 & 프라이버시회복재단(TBYP)

(3) 집단피해대응소비자재단(MDCF)

(4) 네덜란드 개인정보보호 감독기구(AP)

3. 네덜란드 미성년자 개인정보보호 법제 현황

(1) GDPR

(2) 네덜란드 가이던스 및 실행 조치

4. 평가와 시사점

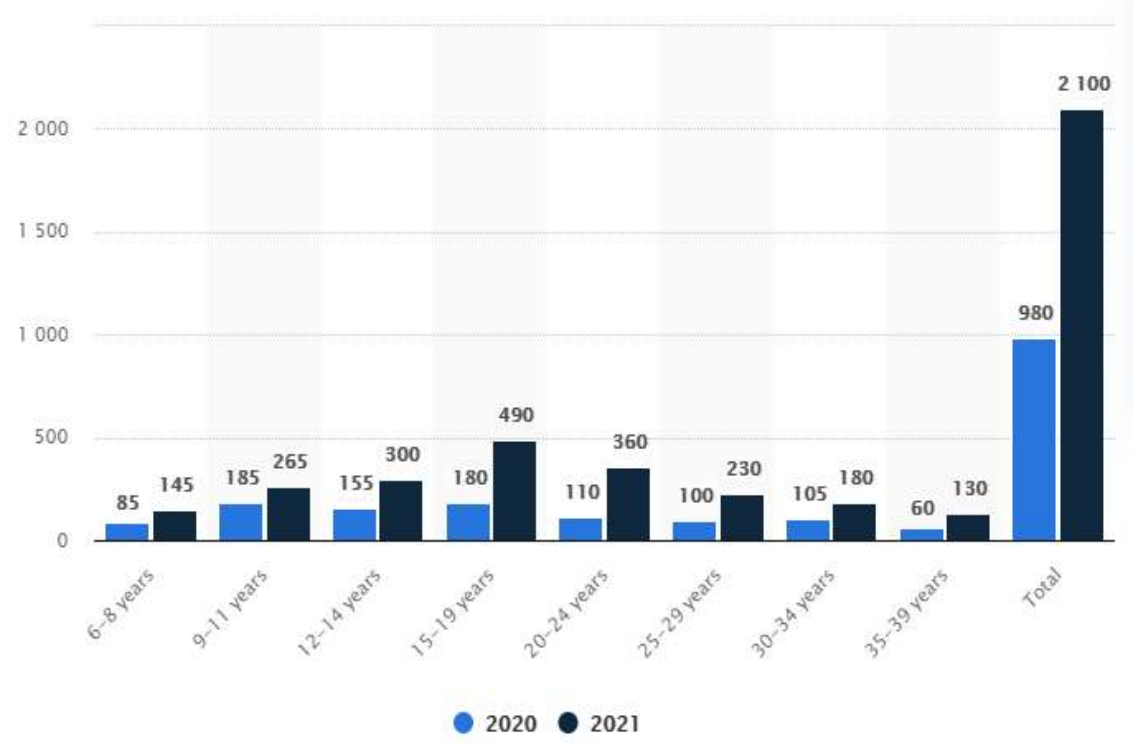
1. 개요

(1) 네덜란드 내 미성년자층을 중심으로 한 틱톡 서비스 성장

▶ 글로벌 동영상 소셜 플랫폼인 틱톡(Tiktok)[2)]이 네덜란드 내에서 아동과 청소년 사이에서 온라인 소통을 위한 주요 매체로 정착

- 틱톡은 미국에 본사를 둔 중국계 IT 기업 바이트댄스(ByteDance)가 제공하는 서비스로 네덜란드 내에서는 '21년 이용자 수가 전년 98만 명 대비 114.3%가 늘어난 210만 명을 기록
- '21년 기준 전체 네덜란드 틱톡 이용자 중 19세 이하 미성년자 수는 총 120만 명으로 전체 이용자 중 과반이 훨씬 넘는 57.1%를 차지
- 특히 15~19세 청소년의 경우 1년 간 2.7배가량이 늘어난 49만 명으로 가장 큰 폭의 성장률과 가입자층을 기록

그림1 _ 네덜란드 연령대별 틱톡 서비스 이용자 변화: 2020-2021 (단위: 천명)



출처: Statista(2021)

2) 중국계 IT기업 바이트댄스(ByteDance)가 2016년 출시한 글로벌 숏폼 모바일 동영상 플랫폼. 이용자들은 15초~3분짜리 짧은 동영상을 제작해 다른 이용자들과 공유할 수 있음. 전 세계 10억 명 이상의 이용자를 보유하고 있으며 주로 10대 청소년층에서 인기가 높음

(2) 네덜란드 내 틱톡 서비스의 개인정보 제재 현황 요약

▶ 네덜란드 내 틱톡 서비스의 급속한 확산과 함께 틱톡의 아동 개인정보보호 규제 위반과 관련된 소송과 과징금 사례도 부쩍 늘어나고 있음

- '21년 6월 이후 현지 주요 소비자단체들은 틱톡이 미성년자의 개인정보를 동의 없이 수집하여 광고 판매에 불법적으로 이용하는 등의 관행에 대해 수십억 유로에 달하는 개인정보보호법 위반 소송을 제기
- 네덜란드의 개인정보 감독기구인 AP(Autoriteit Persoonsgegevens)는 불확실한 개인정보 고지 절차를 지적하며 틱톡에 75만 유로의 과징금을 부과

표1 _ 네덜란드 소비자단체 및 개인정보 감독기구의 틱톡 제재 현황

조직	개인정보 위반 내용				과징금/소송금액	시점
	동의없는 정보 수집	허가없는 국외 정보이전	민감정보 광고활용	정보 활용 고지		
시장정보연구재단(SOMI)	O	O	O	O	17억 유로	2021.6
네덜란드소비자연합&프라이버시회복재단	O	-	O	O	20억 유로+	2021.6
집단피해소비자재단(MDCF)	O	O	O	O	60억 유로	2021.9
네덜란드 개인정보 감독기구(AP)	-	-	-	O	75만 유로	2021.7

출처: 넥스텔리전스(2021)

2. 틱톡의 아동 개인정보보호 위반 소송 및 과징금 사례

(1) 시장정보연구재단(SOMI)

▶ 네덜란드 시장정보연구재단(The Foundation for Market Information Research, 이하 SOMI)은 틱톡이 미성년자 프라이버시 보호와 안전을 위해 충분한 조치를 취하지 않았다며 법원에 제소[3](‘21.6월)

3) DW.com, Dutch parents sue TikTok for €1.4 billion, 2021.6.2.

- SOMI는 틱톡에 대하여 64,000명 부모들의 소송을 대리하여 암스테르담 법원에 총 17억 유로의 소송을 제기

- SOMI는 미성년자로부터 적절한 허가절차 없이 필요 이상의 개인정보를 수집하여 개인화 광고와 함께 아동 개인정보를 미국과 중국으로 이전했다고 주장

- 16세 미만의 청소년과 아동에게 부모의 허가 없이 손쉽게 계정을 생성토록 함으로써 이용자의 적절한 허가 절차를 생략했다고 언급

- 또한, 틱톡은 아동 및 청소년 이용자들이 플랫폼상에서 질식게임(Blackout Challenge)과 같은 위험한 놀이에 가담하는 행위를 방조해 왔다는 점도 지적

※ '21.2월 이탈리아에서는 10세 여아가 틱톡 업로드를 위하여 질식게임의 동영상을 촬영하다가 사망한 사고가 발생한 바 있음

▶ 틱톡은 제소 건에 대해 13~15세 청소년들에게는 비공개(private) 계정을 기본설정으로 처리하여, 팔로우를 승인하지 않은 이용자의 경우 해당 계정의 동영상 시청이 불가능하다고 항변

- 서비스 관리자 역시 주기적으로 부적절한 동영상을 삭제하거나 관련 계정을 중지시키는 활동을 하며 이용자 유해 콘텐츠 발견 시 보고할 수 있는 옵션을 제공해 왔다고 주장

(2) 네덜란드소비자연합 & 프라이버시회복재단(TBYP)

▶ 네덜란드소비자연합(Consumentenbond)과 프라이버시회복재단(Take Back Your Privacy Foundation, 이하 TBYP)은 틱톡에 대해 120~160만 명의 네덜란드 미성년자로부터 불법적인 개인정보 수집 활동을 해 왔다며 총 20억 유로의 소송을 제기[4]('21.6월)

- 두 단체는 개인정보보호법 하에서 미성년자는 각별한 보호를 요하고 있음에도 불구하고 틱톡이 아이들의 프라이버시를 담보로 매년 수백만 유로의 수익을 부당하게 거둬들였다고 주장

- 단체들은 각 피해 미성년자들에 대한 배상금 지급과 함께 그동안 불법적으로 수집해 온 모든 개인정보를 삭제할 것을 요구

- 소송 금액은 피해 배상을 위해 개별 이용자 당 일정 금액 지급(총 20억 유로) 건 외에도 네덜란드 아동의 개인정보를 부당하게 활용해서 획득한 수익에 대해서도 환수를 추가로 요청

4) TBYP, TikTok sued for violation of children's rights, 2021.8.31., AP News, Dutch group launches data harvesting claim against TikTok, 2021.6.25

- 틱톡은 수년간 네덜란드 아동의 개인정보를 불법적으로 수집해 광고 판매에 활용해 왔으며, 수집 개인정보에는 생일, 전화번호, 이메일 주소는 물론 성적 지향성, 종교 및 생체정보(안면인식 등) 등의 민감한 정보도 포함

표2 _ 네덜란드소비자연합&TBYP의 對틱톡 미성년자 이용자당 피해 구제 요구액

13세 미만	13, 14, 15세	16, 17세
1,500유로/이용자	1,250유로/이용자	1,000유로/이용자

▶ 이에 대해 틱톡은 외부 전문가와 조직의 참여를 통해 틱톡 상에서 이용자 개인정보의 안전을 보장하기 위한 다양한 방법을 마련하고 있다고 주장

- 특히 프라이버시 정책, 절차, 적용 기술 면에서 10대 이용자를 위한 각별한 배려를 하고 있다고 언급

(3) 집단피해대응소비자재단(MDCF)

▶ 소비자 보호 단체인 집단피해대응소비자재단(The Mass Damage & Consumer Foundation, 이하 MDCF)은 틱톡이 소비자의 기본권을 대규모로 침해한 것에 대해 집단소송(collective action)에 착수[5](‘21.9월)

- MDCF는 이번 집단소송을 통하여 미성년자뿐만 아니라 틱톡의 모든 이용자들의 권익을 보호하기 위한 차원에서 암스테르담 법원에 틱톡에 60억 달러 이상의 지급 명령할 것을 요구

표3 _ 집단피해대응소비자재단(MDCF)의 對틱톡 이용자당 피해 구제 요구액

6~12세	13~17세	18세 이상
1,750유로/이용자	1,500유로/이용자	1,250유로/이용자

- 또한, MDCF는 틱톡의 행위가 다양한 법과 규정을 위반하고 있으며 특히 틱톡이 사용자 개인 프로필을 광고주와 공유함으로써 소비자의 매우 개인적인 정보를 수집해 왔다는 점에 크게 우려를 제기

5) NL Times, Dutch consumer assoc. claims €1.5 billion in damages from TikTok, 2021.6.24

▶ 재단의 자체 조사에 따르면 개인정보와 관련하여 틱톡은 다음의 사항들을 위반한 것으로 확인

- 별도의 법률적 근거 없이 개인정보를 수집하고 처리
- 사용자에 대해 개인정보 활용에 대해 충분히 투명한 방식으로 고지하지 않음
- 개인정보를 사용자의 허가없이 해외로 전송
- 상세한 소비자 프로필 광고 목적과 자동화된 의사결정에 사용
- 유해 콘텐츠로부터 틱톡 서비스 사용자를 보호하기 위한 장치를 충분히 마련하지 않고 있음

(4) 네덜란드 개인정보보호 감독기구(AP)

▶ 네덜란드 개인정보보호 감독기구(AP)가 미성년자 프라이버시 위반 건으로 75만 유로의 과징금을 틱톡에 부과('21.7월)

- AP는 앱 설치 및 활용 시 대부분 어린 연령대의 네덜란드 이용자에게 틱톡이 제공하는 정보가 영어로만 되어 있으며, 이해하기도 쉽지 않다는 점을 지적
- 즉, 네덜란드어로 프라이버시 방침을 제공하지 않음으로써 틱톡은 앱이 개인정보를 수집, 처리 및 활용하는 방식에 관해 충분한 설명을 제공하지 않았다는 점을 지적
- 틱톡의 이 같은 관행은 이용자가 자신의 개인정보가 어떻게 활용되는지에 대한 명확한 고지를 의무화하는 원칙을 위반한 것

▶ '20년 AP가 틱톡 이용자를 대상으로 한 개인정보 관련 조사에 따르면 일반적으로 아동들은 소셜 미디어상에서 개인정보의 공유행위를 포함한 자신의 행위 결과에 대해 제대로 인지하지 못하고 있는 것으로 나타남

- AP의 틱톡에 대한 강경 조치는 개인정보보호에 취약한 미성년자의 상황을 반영한 것으로, 이들에 대한 제도적인 보호 의무를 강조하고 있는 점을 감독기구가 직접 확인시켜 준 사례

3. 네덜란드 미성년자 개인정보보호 법제 현황

(1) GDPR

▶ **(일반원칙)** GDPR은 아동(children) 개인정보 처리에 따른 특수한 위험성이 존재함을 인정하여, 이에 따른 별도의 보호가 필요하다고 인식(전문 제38조)하고 있으며, 아동을 포함한 모든 개인정보 처리는 다음의 7가지 GDPR 원칙을 준수해야 함(제5조)

① 적법성, 공정성, 투명성의 원칙 (Lawfulness, fairness and transparency)

② 목적 제한의 원칙 (Purpose limitation)

③ 개인정보 처리의 최소화 (Data minimisation)

④ 정확성의 원칙(Accuracy)

⑤ 보관기간 제한의 원칙 (Storage limitation)

⑥ 무결성 및 기밀성의 원칙 (Integrity and confidentiality)

⑦ 책임성의 원칙 (Accountability)

▶ **(개인정보 처리)** GDPR은 정보사회서비스(information society services)[6]와 관련하여 미성년자 개인정보의 적법한 처리를 위해 별도의 부가적인 조건을 제시(제8조[7])

- 서비스 계약 실행을 위해 필요한 처리는 국내법 상 미성년자의 연령을 고려하여 적법한 경우에만 가능

- 컨트롤러나 써드파티의 적법한 이해의 목적에 따라 개인정보 처리를 필요로 하는 경우 미성년자의 개인정보에 대해서는 별도의 고려를 해야 함

  - 정보사회서비스를 16세 미만의 미성년자에게 직접 제공할 경우 개인정보 처리를 위해서는 부모 등 친권 보유자(holder of parental responsibility)의 동의를 의무화

  - 네덜란드에서는 미성년자가 직접 동의 행위를 하기 위해서는 '16세 이상'이어야 하며, 16세 미만인 미성년자의 경우 GDPR에 따라 컨트롤러는 해당 동의가 부모의 감독 하에 이뤄졌음을 입증하기 위한 합리적인 노력을 해야 함

6) information society services(ISS): EU 역내 전자상거래 제도 규정을 위해 만든 개념으로, 2015년 9월에 제정된 Directive (EU) 2015/1535 제1조제(1)항(b)호에서 정의를 밝히고 있음. 해당 정의에 따르면, 동 서비스는 '서비스를 받는 측의 개별 요청에 따라 통상의 영리를 목적으로 원격 지점간에 전자적인 수단을 통해 제공되는 서비스'를 뜻함. 여기에서 원격 지점이란 당사자가 물리적으로 같은 공간에 있지 않은 것을 의미하며, 전자적 수단이란 전자적 장비로 데이터를 처리하여 서비스가 전자적으로 수신자에게 제공되는 것을 의미. 이에 따르면 정보사회서비스는 온라인에서 재화와 용역을 사고파는 전자상거래는 물론 상업적으로 운영되는 모든 웹사이트를 포함. 즉 온라인 광고를 통하여 수익을 창출하는 인터넷 미디어, 검색 광고를 통해 영리를 축하는 검색 엔진 서비스 등이 포함됨
※ 참고: EU 법령 DB https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L1535&from=EN
7) Article 8 GDPR. Conditions applicable to child's consent in relation to information society services

▶ **(투명성)** GDPR은 개인정보 처리에 관한 안내를 '간명하고 투명하며 이해하기 쉬운 형식'과 '접근하기 쉬운 방식'으로 이용자에게 제공해야 하는 '투명성(transparency)'의 원칙을 제시(제12조)

- 투명성은 정보주체의 권리 행사를 지원하고 개인정보 오남용을 막기 위해 반드시 필요한 요건으로서 이를 준수하지 않을 경우 해당 개인정보 처리의 적법성 자체에 문제가 발생

- 이 같은 원칙에 따라, 컨트롤러는 ▲자신, 혹은 대리인의 신원 및 연락처 ▲개인정보 처리의 목적 및 법적 근거 ▲개인정보 수령인 ▲개인정보 해외 이전 관련 사항 ▲개인정보 보관 기간 ▲정보주체의 권리 ▲프로파일링 등 자동화된 의사결정의 유무 등을 '명확하고 평이한 언어'로 설명해야 함

- 특히 아동 이용자를 둔 사업자는 '아동이 쉽게 이해할 수 있는 언어'로 프라이버시 정책을 제시해야 하며(제12조의1)

※ UN의 한 규제 가이던스[8]에서는 어휘, 말투나 스타일 등이 아동에게 적합한 형태로 이뤄져야 할 것을 강조. 즉, GDPR의 투명성 규제 준수를 위해 언급된 아동에 적합한 언어 사용 이외에도, UN 규제 가이던스는 정보가 제시되는 방식과 아동에게 공지할 수 있는 적합한 포맷의 유형과 관련하여 ▲팝업창 ▲3D 터치 ▲마우스를 위로 갖다댈 경우 나타나는 공지문 ▲프라이버시 대시보드 등의 툴을 활용할 것을 권고. 이외에도, 동영상, 스마트폰 또는 IoT 음성 알림, 만화, 애니메이션, 인포그래픽, 플로차트 등 비활자 수단 역시 활용될 수 있다고 제안

(2) 네덜란드 가이던스 및 실행 조치

▶ 현재 AP가 제시하는 국가 단위의 미성년자 개인정보 관련 법제는 별도로 마련되지 않은 상황

- 다만, GDPR 발효 이전 AP는 16세 미만 미성년자의 개인정보가 처리되는 경우 조직은 반드시 부모 동의가 이뤄졌는지 확인할 것을 의무화

▶ '21.3월 네덜란드 정부는 라이덴대학교(University of Leiden)와 신기술 및 문화 연구에 특화된 비영리 연구소인 Waag Society에 의뢰하여 '아동인권 규약(Code for Children's Rights)[9]'을 개발하고 공표함

- 아동인권 규약은 디지털 서비스 개발 시 아동의 권리를 보호코자 하는 기업들에게 다음과 같은 주요 원칙을 가이드로 제공

8) UN Convention on the Rights of the Child in Child Friendly Language
9) https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf

- 디지털 서비스 설계 시 아동의 이익을 가장 우선순위에 둘 것
- 디지털 서비스 설계 시 아동을 참여시키고 이들의 기대치를 반영할 것
- 적법한 방식으로 아동 개인정보를 처리할 것
- 아동이 이해할 수 있고 접근할 수 있는 방식으로 투명성을 담보할 것
- 아동 인권 기반 프라이버시 영향평가를 수행할 것
- 아동 친화적인 프라이버시 설계 방식을 채택할 것
- 아동 개인정보 프로파일링을 피할 것
- 어떤 경우에라도 아동의 경제적인 착취를 방지할 것
- 어떤 경우에라도 아동에게 유해한 서비스 개발을 피할 것
- 산업계 자체적으로 가이드라인을 개발할 것

4. 평가와 시사점

▶ 틱톡은 방대한 가입자 기반과 청소년 중심의 이용자층이 급성장 중임에도 불구하고 가입 및 서비스 이용 절차상 발생되는 아동의 개인정보 처리와 고지의 불투명성으로 인해 전 세계 감독 기관과 소비자 단체로부터 규제 준수 요청이 거세지고 있는 상황

- '19년 미국의 연방거래위원회(FTC)는 13세 미만 아동의 개인정보 수집행위에 대해 '아동온라인프라이버시보호법(Children's Online Privacy Protection Act)' 위반을 들어 틱톡에 570만 달러의 과징금을 부과
  - 미국 소비자단체들은 아동들이 가짜 생일 입력 등을 통해 부모 동의를 얻지 않고 서비스를 가입하여 성인용 앱이나 동영상에 대한 무제한 접근권을 얻음으로써, 틱톡에 의한 불법적인 상업 데이터 활용이나 불법 서비스 계약 체결이 가능하다며 FTC에 추가적인 조사를 촉구
  - 이외에도 미국 정부와 의회에서는 틱톡이 중국 기반 서비스라는 점에서 국가 안보 위기에 대한 우려도 함께 제기되고 있는 상황
- 인도, 영국, EU 등지에서도 틱톡에 대한 유사 소송과 과징금 부과 사건이 이어지고 있는 가운데[10], 국내에서도 '20.7월 틱톡이 개인정보보호 법률을 위반했다는 이유로 1억 8,000만 원의 과징금과 600만 원의 과태료를 부과

10) Republic World, 'After US And India, EU Consumers Accuse TikTok Of Violating User Rights On 'massive Scale'', 2021.2.17

- 방송통신위원회는 틱톡이 법정대리인 동의 없이 만 14세 미만 아동의 개인정보를 수집했다고 판단

- 즉, 만 14세 미만 아동에 서비스를 제공하지 않는다고 고지했지만, 회원 가입단계에서 생년월일을 허위로 입력하거나, 만 14세 이상 항목에 체크하도록 하는 방법으로 나이 확인 절차를 건너뛴 것으로 나타남

- 또한, 개인정보를 국외로 이전할 때 이용자에게 알리고 동의를 받아야하지만, 이 역시 지키지 않은 것으로 확인

▶ 아동층을 주요 대상으로 삼는 소셜 플랫폼 사업자들의 경우 개인정보 사용·처리와 관련한 투명성 및 적법성 원칙 준수를 위한 서비스 설계 및 기술적 보완 대책 수립에 대해 각별한 주의가 필요

• 틱톡과 같이 소극적이고 수동적인 개인정보보호를 위한 절차와 방침을 유지할 경우, 실제 서비스 구현 및 이용 과정에서 발생될 수 있는 고지 불충분이나 동의 하의 정보처리와 관련하여 적법성과 투명성상의 문제에 상시 노출될 수 있음

• 따라서, 소셜 플랫폼 사업자는 법정대리인의 동의가 필요하며 개인정보에 대한 인식이 성숙하지 않은 아동이라는 이용자 특성을 충분히 고려하여, 서비스 설계 단계에서부터 아동의 관점에서 적절한 형식으로 개인정보 처리와 관련된 정확한 정보 제공 방안을 마련할 수 있어야 함

Reference

1. AP News, Dutch group launches data harvesting claim against TikTok, 2021.6.25.
2. DW.com, Dutch parents sue TikTok for €1.4 billion, 2021.6.2.
3. Ministry of the Interior and Kingdom Relations, Code for Children's Rights, 2021.3.
4. NL Times, Dutch consumer assoc. claims €1.5 billion in damages from TikTok, 2021.6.24.
5. Republic World, After US And India, EU Consumers Accuse TikTok Of Violating User Rights On 'massive Scale', 2021.2.17.
6. TBYP, TikTok sued for violation of children's rights, 2021.8.31.,
7. UN Convention on the Rights of the Child in Child Friendly Language

EU의회 싱크탱크의 산업데이터 공유 관련 보고서 분석

[목 차]

1. 개요

EU의회 싱크탱크가 산업데이터(industrial data) 공유 확대를 위한 선결과제를 제시('21.7.7)

2. 산업데이터의 속성, 그리고 개인정보와의 관계

산업 현장에서 생성되는 데이터는 제품, 서비스, 네트워크, 프로세스 관련 데이터뿐만 아니라 사용자나 기타 관계자의 정보도 포함할 수 있음

3. GDPR, 산업데이터 공유 촉진에는 난관으로 작용

산업데이터는 어떤 식으로든 개인정보를 포함하기 쉬우며, 이는 결국 그 데이터의 공유 행위에도 GDPR의 제반 요건이 적용될 수 있음을 의미

4. 기술적 준비와 인센티브도 필요

산업데이터의 B2B 공유 확대를 위해서는 기술적/제도적 기반 마련이 선행돼야 함

5. 마치며

산업데이터 공유 촉진을 위한 입법을 추진할 경우, 그 법이 실효성을 담보할 수 있게끔 산업데이터의 정의부터 명확하게 설정해야 함

1. 개요

▶ EU의회 싱크탱크가 산업데이터(industrial data) 공유에 얽힌 난제들을 조명한 <European Union data Challenge>[11] 보고서를 발행('21.7.28)

- 산업 현장에서 생성되는 데이터는 혁신 촉매로서의 잠재력을 내재하고 있으나 원활한 공유 및 활용을 위한 준비는 부족한 실정
  - '산업데이터'의 엄밀한 정의는 아직 존재하지 않지만, 이렇게 불리는 데이터는 통상적으로 ▲산업 환경에서 구조적으로 수집된 빅데이터의 일부이고, ▲종종 기업 고유 데이터이면서 다양한 유형의 민감정보를 포함
  - 산업데이터는 어떤 식으로든 개인정보를 포함하기 쉽기 때문에 EU 공동의 일반 개인정보 보호법인 GDPR(General Data Protection Regulation)로부터 자유롭기 어렵고, 익명화 같은 비식별화 조치가 늘 유효하다고도 볼 수 없음
- 입법 영역에서는 산업데이터의 공유 및 활용을 지원하기 위한 논의도 진행 중에 있지만, 정책적 개입의 수단과 내용은 실효성을 담보할 수 있는 방향으로 신중히 결정돼야 함
  - 경우에 따라서는 새 법규를 강제하기보다는 기존 규칙을 명확히 설명하는 내용의 연성규범(soft law: 현행법에 준하되 강제성은 없는 가이드라인, 권고, 의견, 선언 등)이나 표준 계약조항을 확산시키는 편이 나을 수도 있고 데이터 표준화 같은 기술적 노력도 필요
- 이에 동 보고서는 산업데이터에 대한 이해를 증진하고 그 활용 촉진에 일조하고자 산업데이터의 개념, 개인정보와의 연관성, 산업데이터 공유의 난제와 선결 조건 등을 개괄

2. 산업데이터의 속성, 그리고 개인정보와의 관계

▶ **(산업데이터의 속성)** EU의 데이터 관련 법과 법안들을 통틀어도 산업데이터의 명확한 정의를 찾아볼 수 없으나, 일반적으로 산업 현장에서 생성되는 데이터는 제품, 서비스, 네트워크, 프로세스 관련뿐만 아니라 사용자나 기타 관계자의 정보도 포함할 수 있음

- 과거에는 이 범주의 데이터를 편의상 '기계 생성 데이터(machine-generated data)'로 지칭
  - EU 집행위원회(European Commission)의 **견해**에 따르면 기계 생성 데이터란 '가상에서든 현실에서든 사람의 직접적인 개입 없이 ▲컴퓨터 프로세스·애플리케이션·서비스나 ▲장비, 소프트웨어, 기계와 연결된 센서에 의해 생성되는 데이터'를 의미

11) 동 보고서는 디지털시대 인공지능 특별위원회(Special Committee on Artificial Intelligence in a Digital Age)의 요청으로 경제·과학·삶의질 정책부(Policy Department for Economic, Scientific and Quality of Life Policies)에서 작성한 것이며 그 내용은 EU의회의 견해와 일치하지 않을 수도 있음

- 비교적 최근에 나온 정책 문서에서는 '기계에 의해 생성된 비개인정보(non-personal machine-generated data)' 정도의 의미로 산업데이터라는 표현이 활용된 것을 볼 수 있으며, EU집행위원회의 유럽데이터전략(European Data Strategy)에서는 '산업 환경에서 생성된 IoT 데이터'를 산업(제조)데이터로 분류

- 그러나 이 같은 종전의 정의나 분류는 산업 현장에서 생성되는 데이터의 특성을 온전히 반영하지 못한다고 볼 수 있는데, 예를 들어 기계 생성 데이터에는 종종 개인정보와 비개인정보가 서로 분리하기 어려운 형태로 혼재돼 있으며, 그 같은 데이터는 제조업 외의 여러 산업 영역에서도 다양하게 생성됨

  - 또한 산업데이터를 비즈니스데이터나 운영데이터와 별개의 것으로 여기는 시각 역시 현실과는 맞지 않는데, 예를 들어 통신업계나 서비스업계(관광, 숙박, 온라인 소매, 물류 등)의 기계 생성 데이터는 그 자체로 기업데이터이자 운영데이터일 수 있음(경우에 따라서는 기업기밀이나 노하우 등도 포함 가능)

▶ **(산업데이터와 개인정보의 관계)** 폐쇄된 산업환경에서 기계에 의해 생성된 데이터라 해도 개인정보를 아예 포함하지 않기는 어려움

- GDPR은 '식별됐거나 식별 가능한 개인과 관련된 일체의 정보'를 개인정보로 정의(GDPR 제4조제1항)하고 있으며, 이처럼 넓은 정의로 인해 '그 자체로는 개인 식별이 불가능하지만 다른 정보와 결합되면 개인 식별이 가능해지는 데이터'까지 개인정보의 범주에 포함됨

  - 따라서 추가 정보 없이는 개인 식별이 불가능하게끔 특정 식별자가 제거된 이른바 '가명정보'에도 GDPR은 적용되며, 그 추가 정보는 기술적/운영적 보호조치를 전제로 별도 보관돼야 함

GDPR 제4조제1항

개인정보(personal data)란 식별됐거나 식별 가능한 자연인('정보주체(data subject)')와 관련된 일체의 정보를 의미한다. 식별가능한 자연인이란 특히 이름, 식별번호, 위치정보, 온라인 식별자 같은 식별정보(identifier)나 신체적, 심리적, 유전적, 정신적, 경제적, 문화적, 사회적 정체성과 연관된 하나 이상의 특징을 참고하여 직접적으로든 간접적으로든 특정 가능한 자연인을 의미한다.

  - 또한 인종, 건강, 성적 지향 등 민감한 영역의 개인정보(GDPR 제9조)는 정보주체의 명시적 동의 등 적절한 법적 근거 없이는 원칙적으로 처리 자체가 불가할 뿐만 아니라 상대적으로 더 높은 수준의 보호 의무를 동반함

- 게다가 데이터 재식별화 위험 등을 고려하면 개인정보와 비개인정보 사이의 구분선은 갈수록 흐려질 것이 유력하고, 이는 결국 후자의 영역이 앞으로 더욱 좁아질 것임을 의미[12)]

  - GDPR은 개인 식별이 불가능하게끔 익명화된 데이터의 처리에는 적용되지 않으나(GDPR 전문 제26항), 익명화 기술이 완벽한 비식별화를 보장할 수는 없음

  - 데이터의 익명화 수준과 유용성은 서로 반비례 관계이기 때문에, 경제적/사회적으로 조금이라도 유용한 데이터를 확보하려면 완벽한 익명화는 불가능하다는 것이 다수 연구자들의 결론

  - 또한 최신 분석기술을 적용할 경우에는 개인정보와 무관해 보이는 데이터에서도 재식별화가 일어날 위험을 배제할 수 없음

3. GDPR, 산업데이터 공유 촉진에는 난관으로 작용

▶ 전술한 바와 같이 산업데이터는 어떤 식으로든 개인정보를 포함하기 쉬우며, 이는 결국 그 데이터의 공유 행위에도 GDPR의 제반 요건이 적용될 수 있음을 의미

- 개인정보와 비개인정보가 데이터 내에 혼합돼 있을 경우, 양자를 분리하는 것이 어렵거나 불가능할 때가 많음

- 그리고 이처럼 개인정보와 비개인정보가 밀접하게 연결돼 있을 경우, 설령 개인정보의 비중이 적더라도 그 혼합 데이터 전체에 대해 GDPR을 적용해야 한다는 것이 EU집행위원회의 입장

- GDPR이 적용되는 개인정보 처리는 적절한 법적 근거(동의 등)를 기반으로 일련의 원칙(목적 제한, 최소화 등)에 따라 이루어져야 함

- 또한 컨트롤러는 GDPR의 정보주체 권리 규정도 준수해야 하는데, 예를 들어 개인정보 이동권(GDPR 제20조) 행사를 보장하기 위해서는 '(정보주체가 제공한) 개인정보를 기계 판독이 가능한 범용 포맷으로 구조화하여 정보주체에게 제공하거나, 해당 데이터를 다른 컨트롤러로 이전할 수 있게끔 지원'해야 함

▶ GDPR은 내용이 매우 복잡한 법이기 때문에 특히 법무 여력이 부족한 중소기업들에게는 데이터 수집 및 공유의 진입장벽으로 작용하기 쉬움

- 예를 들어 위에서 언급한 이동권은 '정보주체가 제공한 개인정보'를 적용 대상으로 하고 있지만, 해당 조문의 자구만으로는 그 실제 범위(IoT/센서 데이터 포함 여부 등)를 가늠하기 어려움

12) 비개인정보는 '개인정보의 여집합'이기 때문에 개인정보의 범위가 넓어질수록 비개인정보의 범위는 좁아짐

- 물론 GDPR은 중소기업의 부담을 덜어주기 위해 직원 규모 250명 미만인 조직에 대해서는 개인정보 처리 활동에 관한 기록 보관 의무(GDPR 제30조)를 면제하고 있으나, 이는 데이터 처리를 상시적으로 수행하지는 않는 업체들에만 적용됨

- 즉, AI 스타트업처럼 데이터 연관성이 큰 업체들은 규모가 작더라도 GDPR의 제반 의무사항을 준수해야 하는 실정이며, 이 같은 EU의 법제는 AI 기반 혁신 확대에 제약 요소로 작용할 수 있음

▶ 또한 GDPR의 적용 범위는 향후 지속적으로 넓어질 수도 있기 때문에 기업들 사이에서는 법적 리스크 원천 차단을 목적으로(혹은 그런 명분으로) 기계 생성 데이터를 아예 공유하지 않는 사례도 나타날 수 있음

• 예를 들어, 원래는 개인정보가 아니었던 데이터라 해도 개인 식별을 위한 추가 정보가 제3자에 의해 결합될 여지가 있다면 EU사법재판소(Court of Justice of the EU)에 의해 개인정보 범주에 추후 편입될 수 있음

• EU는 '데이터의 자유로운 흐름에 관한 규정(Regulation on the free flow of data)'을 통해 회원 각국의 데이터 국내화(data localisation)를 금지하는 등 비개인정보의 원활한 유통을 지원할 방침이나, 동 규정은 '개인정보가 아닌 전자 데이터'를 적용 대상으로 삼고 있기 때문에 개인정보의 범위가 넓어질수록 실효성이 떨어질 수밖에 없는 성격

• 한편, 경우에 따라서는 GDPR 같은 개인정보보호법 외에 지적재산, 저작권, 기업기밀 관련 보호법들 역시 B2B 데이터 공유에 변수로 작용할 여지가 있음

4. 기술적 준비와 인센티브도 필요

▶ 산업데이터의 B2B 공유 확대를 위해서는 기술적/제도적 기반 마련이 선행돼야 함

• 기술적 측면에서는 관련 표준·온톨로지(ontology)[13] 부재와 비용 장벽으로 인해 산업 차원의 데이터 에코시스템이 형성되지 못한 점이 장애 요인

- 가치사슬 구성원 모두가 데이터를 명확하게 이해하려면 공통의 표준과 온톨로지가 필요하지만, 기업들 입장에서는 '기존의 자체 표준을 경쟁사의 표준으로 대체하는 데 대한 거부감'이나 '서로 세대가 다른 IT 솔루션들이 혼재된 환경' 등으로 인해 관련 합의 도출이 어려움

13) 존재하는 사물과 사물간의 관계 및 여러 개념을 컴퓨터가 처리할 수 있는 형태로 표현하는 것. 스탠포드 대학의 그루버(Thomas A. Gruber) 교수는 온톨로지를 '일반적으로 개념화된 것을 형식적으로 명백하게 기술하는 명세(an explicit formal specification of a shared conceptualization)'라고 정의한 바 있으며, 오늘날 온톨로지는 인공지능, 시맨틱 웹, 자연어 처리, 문헌정보학 등 여러 분야에서 지식 처리, 공유, 재사용 등에 활용됨(한국정보통신기술협회 정보통신용어사전 中)

- 설령 기술적 합의가 도출되더라도, 기업간의 데이터 공유를 지원할 새 인프라를 실제 구축하기 위해서는 상당한 규모의 투자가 필요

- 또한 개별 기업 입장에서는 기존 자체 인프라와 새 에코시스템 인프라 사이의 데이터 이동성·상호운용성이 충분히 확보되지 못할 경우 데이터 가용성 측면에서 상대적으로 손해를 보게 된다는 것 역시 부담스러운 부분

• 아울러 현재로서는 기업들의 데이터 공유 의향 자체도 제한적인데, 이는 데이터 공유를 통해 얻을 수 있는 실익이 비용이나 리스크에 비해 크지 않을 수도 있기 때문

- 기업들 사이에서는 일단 데이터를 공유하고 나면 추후 통제할 방법이 없다는 인식이 존재하며, 그로 인한 부담감은 자사 데이터의 잠재적 가치와 기밀성을 스스로 평가하기 어려울 경우에 특히 큼

- 또한 기업 입장에서는 데이터 공유를 통해 호혜적인 결과를 얻을 수 있을 것이라는 확신이 필요

• 한편, 기업간 관계나 데이터의 종류에 따라서도 기업들의 B2B 데이터 공유 의향은 달라질 수 있음

- 수직적 협력관계에서는 밸류체인 내 모든 구성원의 이익을 증진시키는 차원에서 데이터 공유가 적극 추진될 수 있으나, 수평적 경쟁관계인 기업들에게는 상대의 혁신을 위해 굳이 자기 데이터를 제공할 이유가 많지 않음

- 또한 단순히 제품 생산이나 서비스 제공의 부산물로 생성되는 데이터와 별도의 투자(시스템 구축, 설문조사, 베타 테스트 등)가 있어야만 수집할 수 있는 데이터[14]는 기업 입장에서 가치가 다를 수밖에 없음

표1 _ B2B 데이터 공유의 장애 요인

구분	내용
기술적 요인	- 산업 표준 부재 - 데이터 온톨로지의 부재 - 상호운용성 및 이동성 부재
규제 요인	- 법적 불확실성 존재 - 거버넌스 모델 부재 - 데이터 수집 및 공유 관련 인센티브 부재[15]
기업 차원의 요인	- 기술/법무 인력 부족 - 관련 투자 부재 - 노력 부재

14) 많은 비용을 들여야만 확보할 수 있는 데이터를 의무적으로 공유하게 할 경우, 기업들의 데이터 기반 혁신 노력이 오히려 위축되는 부작용을 초래할 수 있음

5. 마치며

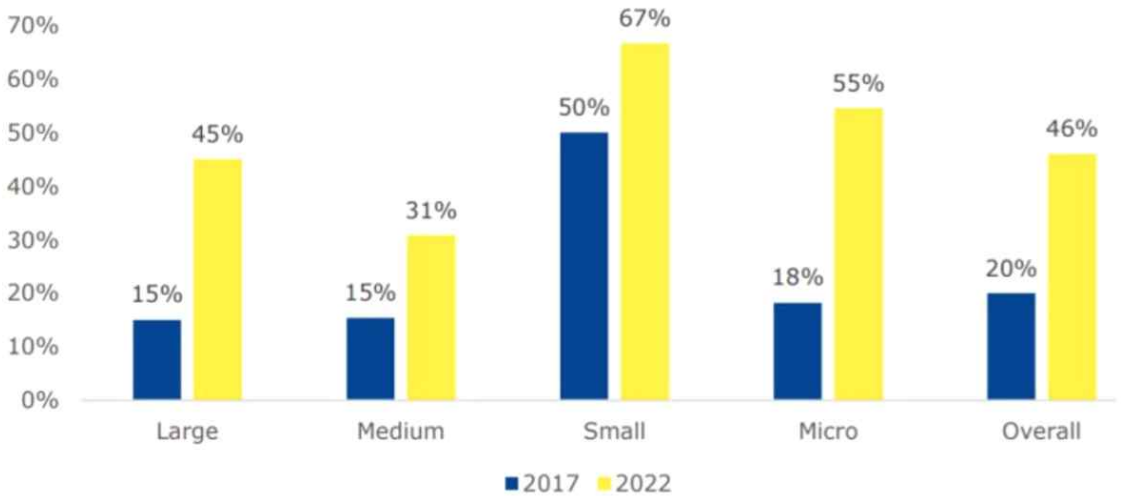
▶ 산업데이터 공유 촉진을 위한 입법을 추진할 경우, 그 법이 실효성을 담보할 수 있게끔 산업데이터의 정의부터 명확하게 설정해야 함

- 부문별로 정책적 개입의 내용을 달리 할 필요도 있는데, 예를 들어 데이터 공유가 이미 시작됐고 기업들의 참여 의지도 높은 부문에 대해서는 일련의 기반 형성 조치(데이터 공유 플랫폼 구축이나 상호운용성 개선 등을 지원)만으로도 충분할 수 있음

- 반면, 데이터 공유 준비가 미진한 부문에 대해서는 그 이유를 우선 파악한 후 적절한 조치를 강구해야 하며, 개인정보 기밀정보가 다량 존재하는 부문에 대해서는 사이버보안 강화 필요성 등을 검토해야 함

- 한편, B2B 데이터 공유 확산을 촉진하기 위한 정책 수단으로는 다양한 유형의 연성규범(soft law)도 유용할 수 있는데, 예를 들어 GDPR의 복잡하고 모호한 부분을 명확히 설명하는 가이드라인/의견 등이 그에 해당

그림1 _ 데이터를 공유하는 기업 비율(기업 규모별 2017년 데이터 vs 2022년 예상치)[16]



- 또한 데이터 상호운용성 등 기술적인 부분의 개선을 위해서는 관련 업계 차원의 자발적인 표준 개발과 모범사례 공유 등이 우선돼야 함

  - 산업 부문별 니즈를 감안해 데이터 공유 관련 표준계약조항이나 법적 가이드를 개발하는 방안도 고려해 볼 수 있으며, 경우에 따라서는 정보 교류 플랫폼 등을 통해 일부 산업 부문의 성과가 여타 부문으로도 확산될 수 있게끔 지원[17]할 필요도 있음

15) EU집행위원회는 신뢰할 수 있는 중개자를 통해 B2B 데이터 공유를 촉진한다는 내용의 데이터거버넌스법(Data Governance Act)을 제안한 바 있으나, 현재로서는 그 구상에 대해서도 기업들이 호응할 이유는 많지 않아 보임
16) Everis, Study on data sharing between companies in Europe, 2018, p. 37.
17) 예를 들어, 어느 산업 부문에서 표준계약조항이 개발됐다면 정보 교류 플랫폼을 통해 이를 여타 산업 부문에도 참고로 제공

Reference

1. European Parliament, European Union data challenge, 2021.7.28
2. European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), 2020.11.25.
3. Official Journal of the European Union, REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018.11.28.

[개인정보보호 동향 보고서 발간 일람]

번호	호수	제 목
1	1월 01	EDPB 제43차 전체회의 주요결과 분석
2	1월 02	GDPR 원스톱 매커니즘에 따른 Twitter의 과징금 부과 사례 분석
3	2월 01	중국 개인정보보호 법제 동향 분석
4	2월 02	ENISA의 가명처리 기술 보고서 주요 내용
5	3월 01	ASEAN 데이터관리프레임워크와 국경 간 데이터 이전 모델계약조항 주요 내용
6	3월 02	개인정보 이동권 관련 주요국 정책 동향 분석
7	3월 03	유럽 인터넷광고협회(IAB)의 서드파티 쿠키 현황과 잠재적 대안 보고서 주요 내용
8	4월 01	프랑스 CNIL의 사회복지 관련 개인정보 처리 기준 주요내용
9	4월 02	주요국 개인정보보호법 준수 비용과 집행 비용
10	5월 01	EU 인공지능(AI) 규제안 주요내용과 개인정보보호
11	5월 02	디지털 소비자 및 개인정보보호 분야 해외 자율규제 적용 현황
12	5월 03	IAB Europe의 정당한 이익 평가(LIA) 수행 가이드 주요 내용
13	6월 01	글로벌 코로나19 백신여권 적용 현황과 개인정보 이슈 및 규제 사례
14	6월 02	유럽사법재판소 개인정보보호 판례집 분석 (1)
15	6월 03	유럽사법재판소 개인정보보호 판례집 분석 (2)
16	6월 04	개정 표준계약조항(SCCs)의 도입배경 및 주요내용
17	7월 01	메타버스 산업 현황과 개인정보보호 이슈 분석
18	7월 02	미국의 개인정보보호법 추진동향
19	7월 03	EDPB, 역외 이전되는 개인정보 보호를 위한 보완조치 관련 권고 발행
20	8월 01	개인정보보호 강화기술(PET) 동향

21	8월 02	안면인식 산업 및 규제 현황과 개인정보보호 쟁점
22	8월 03	EDPB, 음성인식 비서 서비스에 관한 새 가이드라인 발표
23	9월 01	중국 개인정보보호법 제정과 시사점
24	9월 02	네덜란드의 틱톡 규제를 통해 본 아동 개인정보보호 위반 사례 분석
25	9월 03	EU의회 싱크탱크의 산업데이터 공유 관련 보고서 분석

2021

개인정보보호 월간동향분석 제9호

발 행 2021년 9월 30일

발행처 한국인터넷진흥원
개인정보보호본부 개인정보기획팀
전라남도 나주시 진흥길 9
Tel: 061-820-1899

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.