

2023 Privacy Report

개인정보보호 월간동향분석

2월호



2023 Privacy Report

개인정보보호 월간동향분석

2월호

1. 해외 경쟁법 관련 개인정보보호 이슈 분석
2. 미국의 개인정보보호 법제 입법 동향
3. 디지털 자산과 개인정보보호의 관련성 및 고려사항

KISA

해외 경쟁법 관련 개인정보보호 이슈 분석

- 유럽과 미국 사례를 중심으로

[목 차]

1. 개요

2. 유럽: 독일연방카르텔청의 GDPR 해석 시도

- (1) 개요
- (2) 양측 간 소송 진행 상황
- (3) 유럽사법재판소 법무관 의견
- (4) 평가

3. 미국: FTC의 감독 영역 확대

- (1) 개요
- (2) FTC의 페이스북에 대한 규제 절차 돌입
- (3) 평가

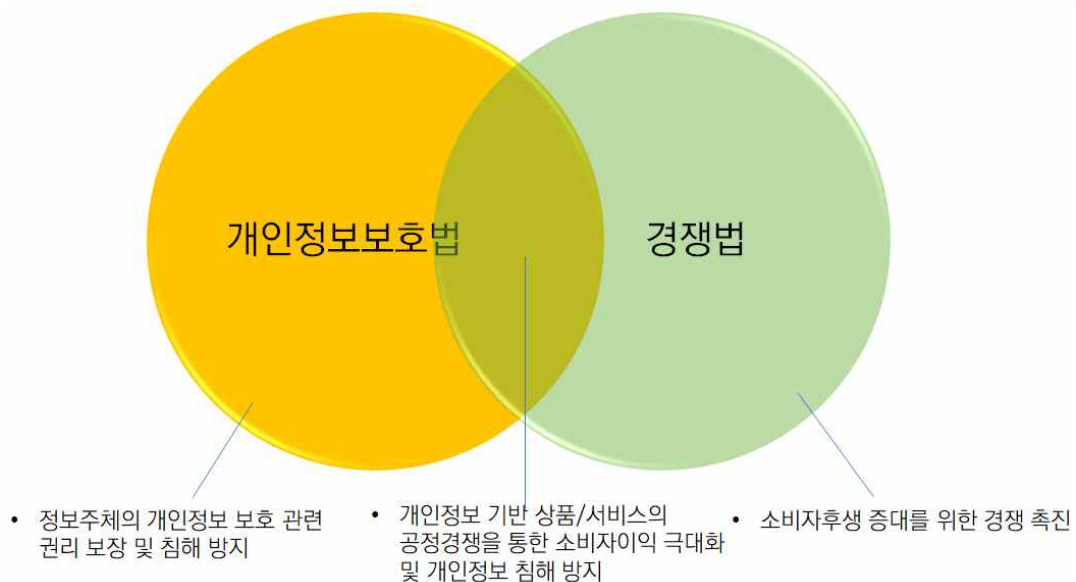
1. 개요

▶ **(서설)** 독점방지 또는 공정경쟁의 판단 기준과 관련한 주요 요소로서 개인정보보호의 중요성이 점차 증가하고 있는 추세

- 경쟁법(competition law)의 오랜 목표는 공정하고 자유로운 경쟁을 통해 적절한 가격을 형성함으로써 소비자후생을 증대하고자 함에 있음
- 그러나, 최근 개인정보보호에 대한 중요성이 높아지고 개인정보의 가치에 대해 재평가가 이루어지면서 비가격적 요소인 개인정보 수집의 독점 방지에 대한 요구가 이어지고 있는 상황
- 이는 시장 지배적 지위를 점하고 있는 회사가 시장 가격의 임의적 형성뿐만이 아니라 개인정보 독점을 통한 반경쟁적 행위를 지속할 가능성이 높다는 것을 의미

- ▶ **(양 법률 간 관계)** 경쟁법과 개인정보보호법은 각각 별도 목적을 위해 제정된 법률로 규제 대상 및 지향하는 목표도 각기 다르나, 최근 두 법 사이에 접점이 발생하는 양상
- 경쟁법은 소비자후생 증대를 위한 경쟁 촉진을 궁극적인 목표로 하고 있는 반면, 개인정보보호법은 개인정보 주체의 개인정보보호 관련 권리 보장과 개인정보 침해 방지를 추구
 - 그러나, 최근에 들어 디지털 기반의 상품 및 서비스가 발달하고 이에 따라 개인정보를 기반으로 한 비즈니스가 호황을 누림에 따라 특정 상황에서는 두 가지 법의 적용이 일부 교차되는 양상을 보임
 - 개인정보를 기반으로 한 디지털 비즈니스인 소셜 네트워크나 온라인 광고 서비스가 시장 독점적 지위를 활용해 개인정보를 무작위로 수집함으로써, 공정한 경쟁에 악영향을 미침과 동시에 개인정보의 무단 혹은 불법적 처리를 초래
 - 상기 위법행위를 규제함에 있어, 시장 지배력 남용 차원에서는 경쟁법 적용이 검토되는 한편, 개인정보 무단 처리에 대해서는 개인정보보호법 적용 가능성이 제기

그림 _ 개인정보보호법 및 경쟁법의 교차 양상



출처 : 토론토대학교 법과대학 유튜브 채널¹⁾, 넥스텔리전스 재구성(2023.2.)

- ▶ **(유형)** 독점방지 또는 공정경쟁과 개인정보보호가 동시에 문제되는 대표적인 유형으로 다음 세 가지 형태가 있음
- 그러나 비즈니스 형태의 진화로 인해 그 유형이 굉장히 다양해지면서도 점점 더 복잡해지는 경향을 보임

1) <https://www.youtube.com/watch?v=zU4FHydTlpI>

표 _ 독점방지/공정경쟁-개인정보보호가 교차하는 주요 형태

유형	세부 내용
(유형1) 소규모 경쟁사 인수	<ul style="list-style-type: none"> • 페이스북의 인스타그램 및 왓츠앱 인수 사례²⁾가 대표적 • 특정 디지털 분야의 시장 지배적 기업이 온라인 광고와 같은 타 부문에서도 지배력을 강화하기 위해, 소규모 경쟁사를 인수함으로써 피인수 기업이 취득한 개인정보 활용 <ul style="list-style-type: none"> - 미래에 발생할 경쟁의 공정성과 이에 따라 소비자가 얻을 수 있는 다양한 이익을 초기에 불가능하게 하는 것으로 공정경쟁에 부정적 영향 - 동시에, 소비자가 기존 피인수기업에 자신의 개인정보를 제공하는 것에는 동의했을지라도, 예기치 못한 인수합병에 따라 인수 기업과 해당 개인정보를 공유하는 것에는 동의하지 않았을 경우 개인정보 보호 문제가 대두
(유형2) 개인정보 대량 취득	<ul style="list-style-type: none"> • 구글의 핏비트(Fitbit) 인수 사례³⁾가 대표적 • 개인정보를 다량 보유한 기업이 마찬가지로 개인정보를 다량 보유한 기업을 인수하여 서비스 확장 <ul style="list-style-type: none"> - 전통적인 반경쟁행위와는 다르나, 개인정보 보유를 바탕으로 시장 진입장벽을 공고히 함으로써 시장 지배력을 확보하는 새로운 형태의 반경쟁적 행위 모델
(유형3) 데이터 유출로 인한 특정당사자 이익 초래	<ul style="list-style-type: none"> • 한 기업이 동종업계 다수 경쟁업체의 서비스와 관련해 데이터 및 개인정보를 집계 및 보유하는 플랫폼 구축 • 플랫폼 기업은 각 기업의 가격책정 정보 또는 경쟁 관련 정보 등 민감정보를 경쟁사 간 상호 비공개로 유지해야 하나, 해당 정보를 유출하여 타 경쟁사가 이로부터 이익을 얻는 경우 경쟁법상 법적 책임을 질 수 있음 • 또한, 하나의 기업에서 취득한 개인정보를 타 경쟁사가 이용할 수 있도록 했다면, 정보주체의 동의 없는 개인정보 처리로서 개인정보 보호 위반 문제도 함께 거론 가능

2) 페이스북은 당시 신생회사로서 잠재적인 경쟁사로 거론되던 인스타그램과 세계 최대 모바일메신저 회사인 왓츠앱을 2012년 및 2014년 순차 인수하면서 소셜 네트워크 시장의 지배적 지위를 얻게 되었는데, 더 나은 개인정보보호 정책을 제공할 수 있는 경쟁사의 출현을 실질적으로 불가능케 함으로써 소비자후생 및 개인정보보호에 관한 권리를 침해

3) 구글과 건강 웨어러블 기기 회사 핏비트는 경쟁사가 아니어서 구글이 핏비트를 인수하더라도 건강 웨어러블 하드웨어 시장에서 구글이 가지는 점유율은 미미한 수준에 불과하므로 공정경쟁에 반하지 않는다고 주장할 수도 있으나, 핏비트가 이용자의 민감정보에 해당하는 건강 개인정보를 다량 보유하고 있다는 점을 고려할 때 인수가 최종 성사될 경우 개인의 민감정보에 대해 구글이 과도한 통제권을 행사함으로써 구글이 이용자의 건강 프로필을 생성하고 그 정보를 구글 광고에 악용할 가능성이 있다는 점에서, 미국 법무부가 기업인수의 공정성에 대해 조사를 진행 중임

- ▶ **(국가/권역 간 접근법 비교)** 독점방지 또는 공정경쟁과 개인정보보호가 교차하는 사안에 대해 유럽과 미국이 접근하는 방식에는 구조적인 차이가 존재
- 유럽 각국은 GDPR 제정 이후 대체로 경쟁당국과 개인정보 감독기관을 별개의 행정 기관으로서 설립 및 운영하고 있어 동일 사안이 개인정보보호법과 경쟁법에 동시 저촉되는 경우 기관 간 법률 적용 및 집행권한이 충돌할 여지가 있음
 - 따라서 공정경쟁과 개인정보보호 이슈가 한 사안에 동시에 나타날 때 어떠한 기관이 해당 문제를 다룰 것인가에 관한 문제가 발생
 - 대조적으로, 미국의 경우 불공정행위 및 반독점행위의 규제를 모두 연방거래 위원회 (Federal Trade Commission, 이하 FTC)가 연방거래위원회법(Federal Trade Commission Act)에 따라 관장하므로 기관 간 권한 충돌 문제가 발생할 여지가 적음

연방거래위원회법 제5조 제(a)항 제2호

연방거래위원회는.....(중간생략).....통상 또는 통상에 영향을 미치는 불공정 경쟁방법의 사용 및 통상 또는 통상에 영향을 미치는 불공정하거나 기만적인 운영방침 또는 행위를 금지할 권한을 가지며 금지하도록 명하여야 한다.

- 더군다나 미국 연방 개인정보보호법이 제정되어 있지 않고, 이에 근거한 개인정보 감독기관이 설립되기 전이어서 원천적으로 FTC와의 집행권한 충돌 문제가 발생할 수 없음
 - 이러한 구조적 차이에도 불구하고 유럽, 미국 모두 독점 및 개인정보 침해 문제를 별개의 사안으로 다루기보다는 특정 사안에서는 두 가지 요소를 하나로 통합해 다룰 필요가 있다는 접근법이 점차 설득력을 얻고 있음
- ▶ 이하에서는 상기 내용을 토대로 개인정보 및 경쟁 이슈가 교차하는 유럽과 미국의 최신 동향을 살펴보고자 함

2. 유럽 : 독일연방카르텔청의 GDPR 해석 시도

(1) 개요

- ▶ 독일연방카르텔청(Bundeskartellamt)이 페이스북에 대해 시장 지배력 남용을 이유로 규제 및 시정 명령을 내리면서 개인정보보호 관련 법률의 일부 조항을 해석
 - 연방카르텔청은 2019년 2월 페이스북(現 메타)에 지배적 사업자로서 GDPR상의 동의 규정을 위반했다고 결정⁴⁾
 - 연방카르텔청은 페이스북이 정보주체의 자발적 동의 없이 제3의 출처에서 개인정보를 수집하는 것을 허용할 뿐만 아니라 페이스북이 소유한 플랫폼(인스타그램, 왓츠앱 등) 간에 이용자 개인정보를 결합하는 것을 허용하는 개인정보 활용 정책을 보유해 왔다고 강조
 - 이에, 현재 형태의 개인정보 처리 정책 보유를 금지하고 연방카르텔청의 GDPR 해석을 준수하도록 하기 위해 12개월 이내에 개인정보보호 및 쿠키 관련 정책을 수정하도록 시정조치를 명령

(2) 양측 간 소송 진행 상황

- ▶ 현재 사건은, 연방카르텔청이 페이스북에 최초 시정조치 명령을 내린 이후 뒤셀도르프 지방 고등법원과 연방대법원을 거쳐, 뒤셀도르프 지방법원에서 유럽사법재판소에 선결적 판결(preliminary ruling)⁵⁾⁶⁾을 요청함으로써 법적 절차가 일시 중단된 상태
 - 페이스북은 연방카르텔청이 개인정보 감독기관의 소관법률인 GDPR에 근거해 집행조치를 할 수 없다고 주장하면서 연방카르텔청의 결정에 불복, 독일 뒤셀도르프 지방 고등 법원(Oberlandesgericht Düsseldorf)에 소를 제기
 - 뒤셀도르프 지방 고등법원은 페이스북의 요청을 받아들여 연방카르텔청의 시정명령에 대해 집행정지 명령을 내렸으나, 이후 연방대법원(Bundesgerichtshof)은 뒤셀도르프 지방 고등법원이 내린 명령을 무효화

4) 이 결정은 경쟁당국이 지배력 남용 평가 시 개인정보보호를 하나의 평가 요소로서 고려했던 유럽 최초의 결정으로, 이전에는 두 가지 법률을 교차점이 없는 별개의 것으로 보는 경향이 강했음. 예컨대, EU집행위원회는 2014년 10월 3일 페이스북의 왓츠앱 인수를 승인하면서, 개인정보보호 이슈가 공정경쟁의 비가격적 매개 변수가 될 수는 있지만 개인정보보호에 대한 우려는 경쟁법이 아닌 GDPR의 보호범위 내에 있는 것이 확고하다는 입장을 밝힌 바 있음

5) 유럽사법재판소가 EU 회원국 법원·재판소의 요청이 있을 때, 유럽연합법의 해석이나 기관들의 행위의 유효성에 관하여 선결적으로 구속력 있는 결정을 내림으로써, 해당 회원국 법원·재판소가 자신의 사건에 판결을 내릴 때 이를 참고할 수 있도록 하는 제도로, 유럽연합법이 전체 회원국에 통일성 있게 적용될 수 있도록 하는 데에 기여

6) Case C-252/21, Meta Platforms Inc., Meta Platforms Ireland 및 Facebook Deutschland GmbH v Bundeskartellamt

- 이에 뒤셀도르프 지방 고등법원은 연방카르텔청이 GDPR 준수 여부를 평가할 자격이 있는지 여부를 결정하고자 법적 절차를 잠시 중단하고 해당 사건을 유럽사법재판소에 회부

(3) 유럽사법재판소 법무관 의견

- ▶ **(서설)** 2022년 9월 20일, 유럽사법재판소의 아타나시오스 란토스(Athanasios Rantos) 법무관은 상기 연방카르텔청 v 페이스북 사건에 대해 뒤셀도르프 지방 고등법원이 회부한 선결적 판결에 관한 의견서를 발표
 - 해당 의견서에서는 뒤셀도르프 지방 고등법원이 질의한 일련의 항목에 대한 법무관의 견해를 밝히고 있으며,
 - 주로 ▲독일 경쟁당국의 GDPR 위반 여부 결정 권한 ▲경쟁당국과 개인정보 감독기관 간의 협력 ▲GDPR 특정 조문에 대한 해석 내용 등이 포함
 - 법무관의 의견은 유럽사법재판소의 결정에 구속력을 미치지 않지만, 통상적으로 유럽사법재판소가 법무관의 의견을 따라 결정을 내리는 경우가 많아 향후 이루어질 재판소의 결정을 미리 예상해 볼 수 있다는 점에서 시사하는 바가 큼
- ▶ **(GDPR 직접적 해석 권한 없음)** 경쟁당국은 GDPR 위반 여부에 대해 직접적으로 입증할 자격을 갖지 않음
 - 경쟁당국은 경쟁법 위반을 이유로 기업을 기소할 때 경쟁법 이외의 기타 법률 위반에 대해서는 판단할 수 있는 권한이 없음
 - 따라서 경쟁당국은 원칙적으로 기업의 GDPR 위반 여부에 대해서는 입증할 수 없음
 - 그러나 경쟁당국이 의심되는 경쟁법 위반행위를 평가함에 있어 문제 사안이 GDPR에 위반되지 않는지 여부를 부차적인 요소로서 고려해 보는 것까지 배제하지는 않음
 - 경쟁당국은 기업의 시장 지배적 지위 남용에 대한 검토 시 GDPR 등 경쟁법 이외의 법률을 예외적으로 검토해 볼 수 있으며,
 - 다만 그러한 행위는 개인정보 감독기관의 해당 규정에 관한 권한을 침해하지 않는 범위에 그쳐야 함
- ▶ **(후순위 집행권한)** 경쟁당국의 집행력이 개인정보 감독기관의 집행권한을 배제하지 못함
 - GDPR과 경쟁법은 다른 목표를 추구하는 것으로, 개인정보 처리와 관련된 행위가 GDPR을 준수하더라도 경쟁법 관련 조항을 위반하는 것이 불가능하지 않음

- 반대로 GDPR을 위반하더라도 그러한 행위가 자동적으로 경쟁법 관련 조항에 반한다고 볼 수 없음
- 따라서 경쟁당국이 GDPR의 해석에 기초하여 기업에 시정 조치 등을 부과하더라도, 다른 영역의 주무당국이 동일한 사실에 대해 관련법에 따라 결정을 내리고 집행하는 것을 막을 수 없음

▶ **(협력 의무)** 경쟁당국은 개인정보 감독기관에 해당 사실을 알리고 협력할 의무가 있음

- 경쟁당국이 GDPR 준수 여부를 평가할 때에는 선임 개인정보 감독기관⁷⁾에 해당 사실을 알리고 협의해야 하며, 특히 이러한 의무는 해당 선임 개인정보 감독기관이 같은 사안에 관해 조사 중일 경우 더욱 발현됨
 - 비록 경쟁당국의 해석이 부수적인 정도에 그치더라도 기관 간 동일한 GDPR 규정에 대한 해석이 달라질 수 있어 GDPR의 균일한 해석을 저해할 수 있기 때문
- GDPR이나 기타 유럽법에는 경쟁법을 적용함에 있어 경쟁당국과 개인정보 감독기관 간의 협력 메커니즘이나 관련 규칙이 존재하지 않지만,
 - 그럼에도 경쟁당국은 EU조약 제4조 제3항⁸⁾에 명시된 협력의무에 따라 행정당국 간 선의로 협력할 의무를 부담
 - 따라서 협력 메커니즘에 대한 명확한 규칙이 없는 경우라도, GDPR 조항의 해석에 관해서는 경쟁당국이 개인정보 감독기관에 정보를 제공하고 협력할 의무가 있음
- 선임 개인정보 감독기관이 특정 행위에 대해 GDPR의 특정 조항을 적용하기로 결정한 경우, 경쟁당국은 해당 조항의 적용 권한을 가진 개인정보 감독기관의 해석을 벗어날 수 없음
 - 경쟁당국은 정보주체의 방어권을 위해 가능한 한 개인정보 감독기관이 채택한 모든 결정을 준수해야 하고, 감독기관이 내린 해석에 대해 의문점이 있는 경우 해당 감독기관과 의논해야 함
- 이와 관련, 경쟁당국이 자체적인 반경쟁행위 조사에 착수하기 전 개인정보 감독기관이 진행 중이거나 진행하려고 하는 조사가 있다면, 특별한 사유가 없는 한 개인정보 감독기관의 조사 결과를 기다리는 등 우선순위를 양보해야 함

7) GDPR 제60조 이하의 원스톱숍 메커니즘에 따라 여러 EU 회원국에 영향을 미치는 범국가적 사안을 다룰 경우 해당 사안의 해결을 주도하는 개인정보 감독기관을 뜻하는 것으로, 주로 다국적기업의 주요 사업장, 지역본부, 본사 소재지 관할국의 개인정보 감독기관이 해당 역할을 담당. 이 사안에서 선임 개인정보 감독기관은 페이스북의 유럽본사가 있는 아일랜드 개인정보 감독기관을 뜻함

8) 성실한 협력 원칙에 따라 유럽연합과 회원국은 완전한 상호 존중을 바탕으로 조약에서 비롯된 임무를 수행하는 데 있어 서로를 지원해야 함

- 본 사안에서 연방카르텔청이 독일 연방 개인정보 감독기관과 협력했다는 사실 및 해당 사건의 선임 개인정보 감독기관인 아일랜드 개인정보 감독기관과 비공식적으로 접촉했다는 사실이 밝혀졌는데, 이는 연방카르텔청이 성실한 협력 의무를 다한 것이라 판단할 수 있음
- ▶ **(GDPR상 동의의 유효성 평가)** 동의의 유효성 및 자발적 동의 제공 여부를 평가할 때에는 기업이 시장에서 지배적 사업자의 지위를 점하고 있는지 여부가 하나의 평가 요소가 됨
- 그러나 시장 지배적 지위에 있는 기업이 해당 지위를 점하고 있다는 사실만으로 정보주체가 제공한 동의가 무조건적으로 무효가 되는 것은 아님

(4) 평가

- ▶ 유럽사법재판소가 법무관의 의견에 따라 결정을 내릴 경우, 경쟁당국과 개인정보 감독기관 모두가 기업의 개인정보보호 운영 방침을 면밀하게 검증할 수 있게 됨
- 다만, 이로 인해 기관 간 상호 체계적인 협력 없이 법률 집행 및 해석의 충돌 여지에 대해 우려하는 일각의 비판이 있음

3. 미국 : FTC의 감독 영역 확대

(1) 개요

- ▶ FTC는 전통적으로 독점방지 및 공정경쟁을 감독하는 행정기관이나, 최근 들어 소비자 개인정보보호에 대한 감시까지 그 집행범위를 확장하는 추세
- FTC는 기업의 시장 지배력 남용을 통한 과도한 가격 인상 등을 감독함으로써 공정경쟁을 위반하는 회사를 주로 조사해 왔는데, 개인정보보호에 대한 검토는 큰 고려사항이 아니었음
- 그러나 최근 FTC의 집행은 시장 지배력을 가진 기업이 개인정보를 어떻게 수집하고 사용하는지 여부에 대한 감독으로 초점이 점차 전환되는 경향을 보임
 - FTC는 연방거래위원회법 제5조에 따라 불공정하거나 기만적인 운영방침 또는 행위를 금지할 권한을 갖는데, 최근 FTC는 동 조항의 '불공정'뿐만 아니라 '기만'에도 중점을 두고 있는 것으로 풀이

- 이러한 경향은 바이든 정부 들어 리나 칸(Lina Khan) 위원장이 부임하면서 더욱 부각되고 있는데, 칸 위원장은 반독점 심사에 있어 공정경쟁과 개인정보보호의 융합적 접근의 중요성을 여러 차례 강조
- 미국은 연방 개인정보보호법 및 별도의 연방 개인정보 감독기관이 존재하지 않으므로 FTC와 개인정보 감독기관 간 집행권한 충돌의 문제가 발생하지 않음
 - FTC 내에서도 경쟁을 담당하는 경쟁국과 소비자 개인정보보호를 담당하는 소비자 보호국의 경계가 벌어지는 추세로,
 - 유럽의 범(汎)기관적 협력 필요성과 유사한 FTC 내 범(汎)부서적 협력 요구가 점차 두드러지고 있음
- 다만, 두 영역의 교차 경향은 최근 들어 나타나기 시작했기 때문에 현재까지 확립된 판례나 성숙된 사례는 존재하지 않음
 - 최근 FTC는 페이스북을 상대로 시장 지배력 남용과 개인정보보호 위반을 동시에 주장하며 규제를 위한 법적 다툼을 벌이고 있는 상황

(2) FTC의 페이스북에 대한 규제 절차 돌입

- ▶ **(서설)** FTC는 반경쟁적 행위를 통해 소셜 네트워크 시장의 독점적 지위를 유지하고 있는 페이스북을 규제하기 위해 워싱턴 DC 지방법원에 소를 제기 (2020년 1월 및 2021년 8월)
 - 해당 소송에서 FTC는 2012년 및 2014년 인수합병이 승인된 인스타그램과 왓츠앱을 페이스북으로부터 매각하도록 명령해 줄 것을 청구
 - FTC는 최초 2020년 1월 소를 제기했으나 이후 증거를 보강해 2021년 8월 재차 소송을 제기했는데, 페이스북의 일일 평균 이용자, 월간 평균 이용자 및 이용자의 평균 사용 시간을 인용하여 페이스북의 시장 지배력에 대한 증거를 강화
- ▶ **(경쟁-개인정보보호 간 통합적 접근)** 특히 재차 제기된 소장에서는 경쟁과 개인정보보호를 융합하려는 FTC 시도가 명확히 나타남
 - FTC는 페이스북의 시장 독점적 지위 유지로 인해 소셜 네트워크 이용자가 고품질 및 다양한 개인정보보호 관련 선택권 등 경쟁이 가져다주는 이점 및 혜택을 박탈당했다고 주장
 - 또한 월등한 개인정보보호 수준을 갖춘 경쟁사와의 경쟁이 존재하지 않아, 페이스북이 경쟁 시장에서 기본적으로 제공했어야 하는 기준선보다 낮은 품질의 개인정보보호 관련 서비스를 제공해 왔다는 의견을 피력

- 이와 같이 페이스북의 불법적인 독점행위가 혁신을 저해하고 이용자 개인정보보호에 부정적 영향을 끼쳤으며, 원치 않는 광고에 이용자를 과도하게 노출시켰다고 비판
- ▶ **(기타 공정경쟁 관련 주장)** 이외에도 FTC는 경쟁을 차단하기 위해 페이스북이 저지른 일련의 행위에 대해 비판을 제기
 - FTC는 페이스북이 인스타그램과 왓츠앱을 인수한 이유가 해당 회사가 페이스북에 잠재적인 위협이 되었기 때문이라고 언급
 - 페이스북 CEO인 마크 저커버그(Mark Zuckerberg)도 2008년 발송한 이메일에서 이들과 경쟁하는 것보다 이들을 인수하는 것이 낫다고 언급했다고 지적
 - FTC는 또한 페이스북이 최고 수준의 개인정보보호 체계를 가진 왓츠앱을 인수함으로써 자사의 성장을 촉진하는 데 도움을 받은 것은 사실이나, 이를 통해 미래의 경쟁 상황을 사전에 차단하는 효과도 누렸다고 주장
- ▶ **(페이스북의 항변)** 페이스북은 FTC의 주장이 설득력이 없을 뿐만 아니라 스스로 한 주장을 입증하지 못하고 있다고 반박
 - FTC는 경쟁 시장에서 소셜 미디어 서비스의 품질 및 개인정보보호 수준의 기준선이 어느 정도인지를 입증하지 못함
 - 즉, 페이스북의 개인정보보호 수준이 낮다는 것을 주장하려면 ▲해당 보호 수준의 통상적인 기준에 대한 입증 및 ▲그 기준보다 개인정보보호 수준이 상당히 낮다는 입증 등 일련의 객관적 입증이 필요함
 - 현재 FTC는 마치 가격 인상폭이 기준선보다 높다는 사실을 전혀 입증하지 못한 채 가격 인상폭을 반경쟁행위의 직접적인 증거라고 주장하는 것과 같음
 - 현재까지 어떤 법원도 FTC가 주장하는 것처럼 각 서비스가 보유한 개인정보의 양을 기준으로 독점력 여부를 판단한 적이 없음

(3) 평가

- ▶ 반독점행위 규제에 개인정보보호 관점을 가미하는 접근법은 소송에서 흔히 받아들여지고 있는 확립된 이론은 아니라는 점에서 소송의 추이를 예단하기 어려움
 - 반독점행위에 대한 판단 시 FTC는 역사적으로 소비자후생과 관련해 비가격적 요소를 고려하는 것을 피하고자 했으나,
 - 현재 FTC는 이용자의 개인정보보호라는 비가격적 요소를 적극적으로 활용하고자 하고 있어, 페이스북의 불공정 경쟁 여부가 법원에서 어떻게 받아들여질지에 대해 귀추가 주목
- ▶ 이와 관련, 비가격적 요소에 대한 모든 입증책임은 규제를 주장하는 원고 FTC가 부담하게 되므로, FTC가 새로운 접근법에 근거해 개인정보보호 수준을 어떻게 수량화하여 입증해 낼 것인지가 법적 다툼의 성패에 관건이 될 것으로 전망

Reference

1. Wilson Sonsini, EU Court Opinion: Competition Authorities May Consider Data Protection Breaches in Their Investigations, 2022.11.10.
2. InfoCuria, OPINION OF ADVOCATE GENERAL RANTOS, Case C-252/21, 2022.9.20.
3. iapp, The thin line between privacy and antitrust, 2020.6.23.
4. Medialaws, AG Opinion on Case C-252/21: The Interplay between Data Protection Law and Competition Law, 2023.2.15
5. Euractiv, EU court adviser: Competition bodies may consider data protection breaches in their probes, 2022.9.26.
6. Mixed, Meta vs. Germany: What has happened so far, 2022.5.5.
7. Fordham University School of Law, Is Privacy an Antitrust Issue? A Growing Movement, 2020.4.1.
8. Law.com, FTC's Move to Link Data Privacy With Antitrust Has Attorneys Waiting for Clarity, 2022.9.13.
9. Digiday, Facebook fights FTC's new privacy themes in revised antitrust case, 2021.10.7.
10. Constantine Cannon, FTC Chair Khan Squares the Circle With an "Interdisciplinary Approach" to Protecting Privacy and Competition, 2022.4.21.
11. DuaneMorris, Preparing for a New Era of Consumer Privacy in Antitrust Enforcement, 2021.12.17.
12. Protocol, The FTC's antitrust case against Meta could be great for privacy, 2022.1.26.
13. npr, Judge allows Federal Trade Commission's latest suit against Facebook to move forward, 2022.1.11.
14. Global Counsel, The FTC fuses competition, privacy, and consumer protection concerns to open a new front against Big Tech, 2022.10.7.

미국의 개인정보보호 법제 입법 동향

[요약]

1. 개요

미국에서는 '22.6월 연방 개인정보보호법안(ADPPA)가 발의되었으나 의회 통과 여부는 아직 불확실하며 주 차원에서 활발한 입법 움직임이 이어짐

2. 미국 주요 주의 개인정보보호 관련 입법 동향

- (1) **(캘리포니아주)** 소비자 개인정보보호법(CCPA)을 개정·강화한 개인정보보호관리법(CPPRA)을 '23.1월부터 시행
- (2) **(버지니아주)** 소비자 개인정보보호법(VCDPA)을 제정하여('21.3), '23.1월부터 시행
- (3) **(콜로라도주)** 개인정보보호법(CPA)을 제정하여 '23.7월부터 시행 예정
- (4) **(유타주)** 소비자 개인정보보호법(UCPA)을 제정하여 '23.12월부터 시행 예정
- (5) **(코네티컷주)** 개인정보보호법(CTDPA)을 제정하여 '23.7월부터 시행 예정
- (6) **(기타 주)** 인디애나, 아이오와, 하와이, 켄터키주 등 '23.2월 초 기준 16개 주에서 개인정보 보호 관련 법안이 발의됨

3. 결론 및 시사점

미국 연방 및 주별로 개인정보보호 입법화가 활발히 추진됨에 따라 미국에서 활동하거나 미국 소비자 정보를 수집, 처리하는 한국 기업들의 대비 필요

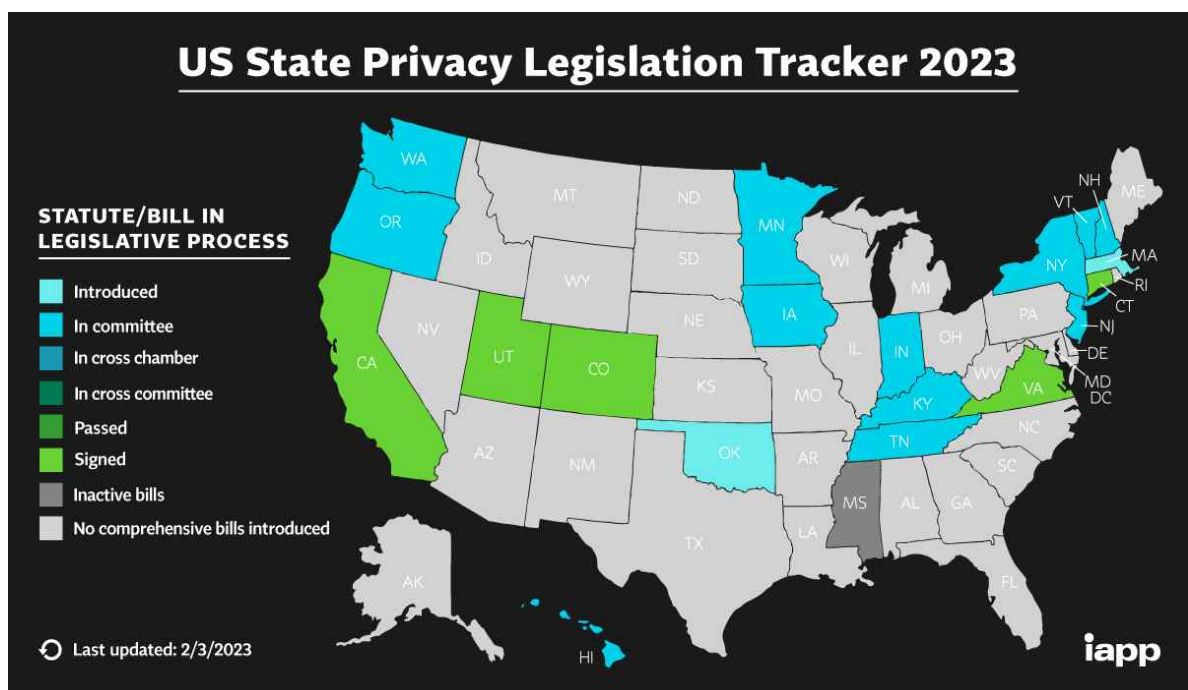
1. 개요

- ▶ 미국에서는 아직 연방 차원의 포괄적인 개인정보보호법은 제정되지 않았으나 '22.6월 미국 의회의 양당 의원들이 연방 개인정보보호법안*(ADPPA)을 발의

* American Data Privacy and Protection Act, ADPPA

- ADPPA는 ▲개인정보 최소화 ▲투명성 ▲17세 미만 아동·청소년 대상 표적 광고 금지 ▲민감 정보 수집 시 명시적 동의 ▲대규모 개인정보처리자의 경우 영향평가를 수행하고 그 결과를 FTC(연방거래위원회)에 보고하는 등의 내용을 포괄
- ▶ 주 차원의 개인정보보호법 입법화 역시 활발히 진행되고 있으며, 특히 올해에는 캘리포니아주를 포함한 여러 주에서 새로운 개인정보보호법이 시행됐거나 시행 예정
 - 캘리포니아주는 '23.1월부터 소비자 개인정보보호법(CCPA)*을 대체하여 한층 강화된 개인정보보호권리법(CPPRA)*을 시행
 - * California Consumer Privacy Act ** California Privacy Rights Act
 - 버지니아주는 '23.1월부터 소비자 개인정보보호법(VCDPA)*을 시행
 - * Virginia Consumer Data Protection Act
 - 콜로라도주와 코네티컷주는 '23.7월부터 각각 개인정보보호법 CPA*와 CTDPA**을 시행 예정
 - * Colorado Privacy Act ** Connecticut Data Privacy Act
 - 유타주는 12월 31일부터 소비자 개인정보보호법(UCPA)*을 시행 예정
 - * Utah Consumer Privacy Act
 - 이외에도 미국 16개 주*에서 개인정보보호 법률이 발의되어 입법화 시도
 - * 인디애나, 아이오와, 하와이, 켄터키, 메릴랜드, 매사추세츠, 미네소타, 뉴햄프셔, 뉴저지, 뉴욕, 오클라호마, 오리건, 테네시, 텍사스, 버몬트, 워싱턴 주

그림 미국 주 차원의 개인정보보호 입법화 추진현황9)



출처: IAPP

9) <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

2. 미국 주요 주의 개인정보보호 관련 입법 동향

(1) 캘리포니아주

- ▶ 미국에서 처음으로 '소비자 개인정보보호법(CCPA)'을 제정하여('18.12), '21.1월부터 시행에 들어간 캘리포니아주는 CCPA의 조항을 개정·강화한 '개인정보보호관리법(CPRA)'을 제정하고('20.11) '23.1월부터 시행
- CPRA는 CCPA와 비교하여 ▲개인정보보호 원칙 추가 도입 ▲민감정보에 대한 새로운 정의 및 처리 제한 ▲소비자의 권리 확대 ▲기업의 의무와 책임성 강화 ▲새로운 개인정보보호 집행기관의 설립 등의 내용을 새롭게 포함
- CPRA의 적용 대상은 캘리포니아 거주자의 개인정보에 접근하여 이용하는 기업으로 ①연 매출이 2,500만 달러 이상이거나 ②소비자 개인정보를 10만 건 이상 보유하거나 ③개인정보 판매 및 공유에 따른 매출이 총매출의 50% 이상을 차지하는 경우임
- 기존 CCPA에서는 5만 건 이상 개인정보를 보유한 기업에 법률을 적용했으나 CPRA는 기준을 10만 건 이상으로 상향 조정하여 소규모 사업자들은 적용 대상에서 제외

표1_ CPRA의 주요 변화

구분	주요 내용
적용 대상의 축소	<ul style="list-style-type: none"> 소규모 사업자중 연간 5~10만 명의 개인정보를 보유한 사업자를 적용 대상에서 제외
개인정보보호 원칙의 추가	<ul style="list-style-type: none"> GDPR의 개인정보 처리 원칙 중 데이터 최소화 원칙, 목적 제한의 원칙, 보유기한 제한 원칙을 조문에 반영 동의 기준(Consent Standard) 개념의 확대 적용
민감정보의 규정	<ul style="list-style-type: none"> 개인정보에서 민감정보의 개념을 분리하고 민감정보의 공개와 활용을 엄격히 제한 민감정보는 △사회보장번호, 운전면허번호, 주 ID 번호, 여권번호 △비밀번호를 사용한 계정 로그인 정보 △정확한 위치 정보 △인종·민족, 종교, 조합 가입 관련 정보 △유전자 정보와 생체 정보, 건강 분석 정보 △성생활과 성적 지향 등을 포함
소비자의 권리 강화	<ul style="list-style-type: none"> 부정확한 정보에 대한 정정 요구권, 공유 거부권, 자동화된 의사결정 거부권 등의 소비자 권리를 추가로 보장하고 개인정보 무단 열람, 유출, 도난 사고 발생 시 정보주체의 대응 범위를 확대
기업의 의무와 책임성 강화	<ul style="list-style-type: none"> 소비자 개인정보 판매 또는 공개 시 계약의 의무, 개인정보 보안 의무, 고위험 활동에 대한 개인정보 영향평가 및 보안 감사의 의무 추가
개인정보보호 감독기구 신설	<ul style="list-style-type: none"> 캘리포니아주 개인정보보호 감독기구(California Privacy Protection Agency)를 신설하여 법률 위반에 대한 조사, 행정처분, 규칙 공포 등의 권한을 부여

출처: 넥스텔리전스(주) 정리

(2) 버지니아주

- ▶ 버지니아주는 미국에서 두 번째로 개인정보보호 관련 '소비자 개인정보보호법(VCDPA)¹⁰⁾'을 제정하고('21.3), '23.1월부터 시행
 - 버지니아 주민을 대상으로 사업을 수행하거나 제품·서비스를 제공하면서 연간 10만 명 이상 소비자의 개인정보를 처리하거나, 총매출 중 개인정보 판매 부문이 50% 이상이면서 최소 2만 5천 명의 개인정보를 취급하는 사업체를 대상으로 법률 적용
- ▶ VCDPA는 소비자의 권리 및 컨트롤러와 프로세서의 의무사항을 규정하며, CPRA와 유사점이 많으나 일부 차이도 존재
 - VCDPA는 소비자에 알 권리, 접근권, 정정권, 삭제권, 개인정보 이동권, 개인정보 판매 거부권에 더해 타겟 광고 거부권, 프로파일링 거부권 등을 부여
 - VCDPA는 컨트롤러의 의무로 개인정보 처리 최소화, 보안 조치, 민감정보 처리 금지, 정보주체에 대한 차별 금지, 정보주체의 권리 행사에 대한 이행 기간 준수(45일) 등을 규정하며, 표적 광고 또는 프로파일링을 위한 개인정보 처리 등 특정 유형의 처리 활동에 대하여 개인정보 영향평가를 의무화
 - VCDPA는 CPRA와 달리 개인정보 감독기구에 관한 규정이 없으며, 주 법무장관(검찰총장을 겸임)에 집행권한을 부여
 - 위반 건당 최고 2,500달러(고의적 위반 시 7,500달러)의 벌금을 규정한 CPRA와 비교해 VCDPA는 건당 최고 7,500달러의 벌금을 부과

(3) 콜로라도주

- ▶ 콜로라도주는 미국에서 세 번째로 개인정보보호법(CPA)¹¹⁾을 제정하고('21.7), '23.7월부터 시행 예정
- ▶ CPA는 소비자의 권리로 소비자 자신의 개인정보 처리 거부(Opt Out), 접근, 정정, 삭제, 개인정보 복사본 획득 등을 규정하며, 컨트롤러와 프로세서의 의무사항 규정
 - 컨트롤러가 소비자의 권리 주장, 투명성, 목적 명시, 개인정보 최소화와 부차적 사용 방지, 불법적인 차별 방지 등 의무사항을 충족할 방법을 규정

10) General Assembly of Virginia, Consumer Data Protection Act, 2021.3.2.

11) The State of Colorado, Concerning Additional Protection of Data Relating to Personal Privacy, 2021.7.7.

- 컨트롤러가 표적 광고, 프로파일링, 개인정보 판매, 민감한 개인정보 처리 등 소비자 피해 위험이 높은 개인정보 처리 활동에 대해 개인정보보호 평가를 수행하도록 규정
- ▶ CPA는 캘리포니아 및 버지니아주의 개인정보보호법과 유사하지만 일부 차이도 존재
 - CPA는 특정 요건을 충족하는 비영리 단체에 법률이 적용되는 반면 캘리포니아 및 버지니아의 법률은 비영리 단체에 대해 적용하지 않음
 - 캘리포니아 법률과는 다르지만 버지니아의 법률과 유사하게 CPA는 직원이나 B2B(Business-to-Business) 거래에 적용되지 않으며, 개인 소송 권한을 부여하지 않음
 - CPA는 컨트롤러에게 하위 프로세서에 대한 감사 권한, 삭제 권한 및 이의 제기 권한 등을 포함하여 법령에 따른 프로세서에 대한 의무를 부과

(4) 유타주

- ▶ 유타주는 미국에서 네 번째로 소비자 개인정보보호법(UCPA)을 제정하고('22.3) '23.12월 31일부터 시행 예정
 - UCPA는 상당 부분 버지니아의 VCDPA를 토대로 마련되었으며 콜로라도와 캘리포니아의 개인정보보호법과 일부 유사점이 있으나 상대적으로 사업자 친화적인 것으로 평가됨
 - UCPA는 유타 주민을 대상으로 사업을 수행하거나 제품·서비스를 제공하며 연간 매출이 2,500만 달러 이상의 사업체 중 연간 10만 명 이상 소비자의 개인정보를 처리하며, 총매출 중 개인정보 판매 부문이 50% 이상이면서 최소 2만 5천 명의 개인정보를 취급하는 사업체를 대상으로 적용됨
- ▶ UCPA는 소비자의 권리와 컨트롤러 의무를 규정하고 있으며, 개인정보 감독기구를 설립하지 않고 주 법무장관에게 법 집행 권한을 부여
 - UCPA는 소비자의 권리로 알 권리, 접근권, 삭제권, 개인정보 이동권, 개인정보 판매권 등을 부여하나 정정권에 대한 명시적 규정은 없음
 - 컨트롤러는 개인정보 처리 최소화, 보안 조치, 정보주체에 대한 차별금지, 정보주체의 권리행사에 대한 이행 기간 준수(45일) 등의 의무를 준수해야 하며, 민감정보 처리 전 소비자에게 명확한 통지 및 옵트아웃 기회를 제공해야 함
 - 법률 위반 시, 주 소비자 보호 부서에서 1차로 위반행위에 대한 조사 권한을 행사한 뒤 법무장관에 사안을 회부

(5) 코네티컷주

- ▶ 코네티컷주는 미국에서 다섯 번째로 개인정보보호법(CTDPA)¹²⁾을 제정하고 '23.7월부터 시행 예정
 - 코네티컷 주내에서 사업 활동을 하거나 코네티컷 주민을 대상으로 상품·서비스를 제공하면서, 10만 명 이상의 소비자 개인정보를 취급하거나, 총매출 중 개인정보 부문이 25% 이상이면 최소 2만 5천 명의 개인정보를 취급하는 사업체를 대상으로 함
- ▶ CTDPA는 소비자의 권리와 컨트롤러의 의무사항, 민감정보 관련 내용 등을 규정
 - 소비자는 접근권, 정정권, 삭제권, 이동권 등의 권리와 함께 광고 타겟팅과 개인정보 판매, 자동화된 의사결정 등 특정 목적의 개인정보 처리에 대한 거부권을 보유
 - 컨트롤러는 처리되는 개인정보의 종류, 개인정보 처리 목적, 소비자의 권리 행사 방법, 제3자와 공유하는 개인정보의 종류 및 제3자의 유형, 실제 활용 가능한 연락처 등을 의무적으로 고지해야 함
 - 컨트롤러는 설계에 의한 개인정보보호, 개인정보 수집 최소화, 개인정보의 목적 외 활용 금지, 적정 보안 조치의 수립과 이행 등의 원칙을 준수해야 하며, 민감정보의 처리를 위해서는 당사자로부터 법적으로 유효한 사전 동의를 얻어야 함
- ▶ CTDPA는 규정 위반에 대한 법 집행 권한을 법무장관에게 부여하며 소비자에게 사적 소송권은 부여하지 않음
 - '23년 7월 1일과 '24년 12월 31일 사이에 코네티컷주 법무장관으로부터 규정 위반 혐의를 고지 받은 사업자에게는 60일의 시정 기간이 부여되며 '25년 1월 1일부터는 법무장관 재량으로 시정 기회 부여 여부를 결정 가능

표2_ 유타주 UCPA와 코네티컷주 CTDPA의 비교

구분	주요 내용
적용 범위	<ul style="list-style-type: none"> • UCPA와 CTDPA 모두 비영리법인에는 적용되지 않음 • UCPA는 연매출 2,500만 달러 이상의 사업체로 적용 범위를 한정
정보 주체의 권리	<ul style="list-style-type: none"> • UCPA와 CTDPA 모두 소비자에게 알 권리, 접근권, 삭제권, 이동권, 개인정보 판매 거부권 등을 부여 • CTDPA는 UCPA에 없는 정정권 및 타겟 광고 거부권, 프로파일링 거부권을 추가로 규정

12) CT.gov, The Connecticut Data Privacy Act, 2022.5.10.

구분	주요 내용
컨트롤러의 의무	<ul style="list-style-type: none"> • UCPA와 CTDPA 모두 개인정보 처리 최소화, 보안 조치, 정보 주체에 대한 차별금지, 정보주체의 권리행사에 대한 이행 기간 준수 등을 규정 • 민감정보 처리 시 UCPA는 소비자의 동의를 요구하지 않고 처리 전 소비자에게 명확한 통지 및 옵트아웃 기회 제공을 규정한 데 비해, CTDPA는 소비자의 동의를 받도록 규정 • UCPA는 개인정보 영향평가에 대한 규정이 없으나 CTDPA는 소비자에게 해를 끼칠 위험이 높은 처리 활동에 대하여 영향평가의 필수 이행 및 문서화를 요구
개인정보 감독기구 및 집행	<ul style="list-style-type: none"> • UCPA와 CTDPA 모두 개인정보 감독기구 설립 없이 주 법무장관에게 집행권한을 일원화

출처: 넥스텔리전스(주) 정리

(6) 기타 주의 개인정보보호 입법 동향

▶ (인디애나주) 소비자 개인정보보호에 관한 법안 SB 5가 상원을 통과('23.2월)

- 하원 심의를 남겨둔 SB 5는 버지니아주의 개인정보보호법과 유사하며, 거래 규제에 관한 주법을 개정하여 개인정보를 다루는 민간 사업체에 대한 개인정보보호 요구사항을 강화하는 내용을 골자로 함
- 법안에 따르면 소비자가 원하는 경우 기업에 자신의 개인정보를 DB에서 삭제하도록 요구함으로써 침해가 일어나기에 앞서 소비자 스스로 보호 가능

▶ (아이오와주) 유타주의 소비자 개인정보보호법과 유사한 House Study Bill 12가 경제 성장 및 기술 분과위원회를 통과('23.1월)

- 동 법안과 같은 내용의 법안이 지난해 아이오와주 하원을 통과했으나 상원에서 부결된 바 있으며, 올해는 1월 23일 상원에서 동반 법안이 Senate Study Bill 1071이라는 이름으로 발의됨
- 동 법안은 사업자 친화적인 유타의 UCPA와 유사하게 소비자의 권리 중 정정권이 포함되지 않으며, 민감정보 수집 시 정보주체의 동의가 아닌 통지 및 옵트아웃을 요구

▶ (뉴욕주) 개인정보보호법안(New York Privacy Act, SB 365)이 상원에서 발의되어 소비자 보호위원회에서 심의 중('23.1월)

- 동 법안은 기업이 개인정보에 대한 비식별 처리 방법을 공개하고 데이터 공유와 관련된 특별 보호조치를 마련할 것과 소비자에게 개인정보를 공유하는 모든 사업체의 이름을 알릴 것을 요구

- ▶ **(매사추세츠주)** 연방 ADPPA를 토대로 한 개인정보보호법(Massachusetts Data Privacy Protection Act, MDPPA)이 상원과 하원에서 발의됨('23.1월)
- 한편, 정보 프라이버시 및 보안법(Massachusetts Information Privacy and Security Act, MIPSА)도 상원과 하원에서 발의됨
- ▶ **(기타)** 일리노이주에서는 개인정보의 공개와 접근권에 초점을 둔 '알 권리 법안(Right to Know Act, HB 1381)'이 발의되었으며, 미네소타주에서는 상원에서 개인정보 수집 시 동의를 요구하는 SF 950이 발의됨('23.1월)

3. 결론 및 시사점

- ▶ 미국은 연방 차원의 일반법이 없는 가운데 '22.6월 미국 의회의 양당 의원들이 발의한 연방 개인정보보호법(ADPPA)은 최근 몇 년간 발의된 관련 법안 중 초당적 지지를 얻으며 통과 여부에 관심이 쏠림
- '22.7월 하원 에너지 및 상업위원회는 ADPPA의 수정 법안을 통과시켰으며 '23.1월 출범한 제118대 의회에서 ADPPA에 대한 논의가 이루어질 전망
- 주 개인정보보호법은 서로 차이점이 있어 기업이 이를 모두 준수하기가 까다로운 만큼 미국 전역에 일괄 적용될 수 있는 연방법에 대한 폭넓은 공감대가 형성되어 있음
- 그러나 의회 내부적으로는 법안의 범위와 집행 방식 등에서는 여전히 이견이 존재하여 법안 통과 가능성은 미지수
- ▶ 연방법 입법이 지지부진한 사이, 주 차원의 개인정보보호 입법화는 캘리포니아주를 시작으로 5개 주에서 이미 제정이 완료됐으며, 올해 들어 여러 주에서 새로운 법안을 발의하는 등 활발한 흐름을 보임
- 캘리포니아주와 버지니아주에서는 '23.1월부터 새로운 개인정보보호법이 시행되었으며, 콜로라도주와 코네티컷주는 '23.7월부터, 유타주는 '23.12월부터 시행 예정으로 기타 여러 주에서 개인정보보호 입법화를 추진 중

표3_ 미국 주의 개인정보보호법 발의 및 입법 현황('22.2.10 기준)

입법 추진 현황	해당 주
제정 완료(5)	<ul style="list-style-type: none"> • 캘리포니아주('18.6월) • 버지니아주('21.3월) • 콜로라도주('21.7월) • 유타주('22.3월) • 코네티컷주('22.5월)
의회 논의 중(16)	<ul style="list-style-type: none"> • 하와이주(소관 위원회) • 아이오와주(소관 위원회) • 인디애나주(상원 통과) • 켄터키주(소관 위원회) • 메릴랜드주(법안 발의) • 매사추세츠주(법안 발의) • 미네소타주(소관 위원회) • 뉴햄프셔주(소관 위원회) • 뉴저지주(소관 위원회) • 뉴욕주(소관 위원회) • 오클라호마주(소관 위원회) • 오레곤주(소관 위원회) • 테네시주(소관 위원회) • 텍사스주(법안 발의) • 버몬트주(소관 위원회) • 워싱턴주(소관위원회)
폐기 (1)	<ul style="list-style-type: none"> • 미시시피주

출처: 넥스텔리전스(주) 정리

▶ 미국의 주 차원 개인정보보호 법령은 EU GDPR과 상당 부분 유사한 점이 있으나, 주별로 일부 차이가 있으므로 미국에서 활동하거나 미국 소비자의 개인정보를 수집 및 처리하는 기업들은 활동 지역의 법령에 유의하여 준수 방안을 마련할 필요가 있음

- 캘리포니아주의 CPRA는 개인정보 처리·통제하는 사업체를 서비스 제공업체, 계약업체 등으로 정의하나, 버지니아와 콜로라도, 유타, 코네티컷 주는 EU GDPR과 동일한 컨트롤러, 프로세서 명칭을 사용하고 유사한 조항을 포함하는 것 등에서 차이 존재

Reference

1. DataGuidance, USA: State privacy laws entering into effect in 2023, 2023.1.
2. Digital Guardian, Indiana Plotting Data Privacy Laws of Its Own: Senate Bill 5 and SB 358, 2023.2.1.
3. Holland & Knight, United States: Data Privacy And Security Report: January 2023, 2023.2.6.
4. JD SUPRA, Connecticut Set to Become Fifth State With a Comprehensive Privacy Law, 2022.4.28.
5. JD SUPRA, Proposed State Privacy Law Update: January 30, 2023, 2023.1.30.
6. IAPP, US State Privacy Legislation Tracker, 2023.2.10.
7. IAPP, Utah becomes fourth US state to enact comprehensive consumer privacy legislation, 2022.3.25.

디지털 자산과 개인정보보호의 관련성 및 고려사항 - CIPL의 검토 내용

[목 차]

1. 배경
2. 블록체인의 특성과 유형
3. CIPL 회의에서의 주요 논의 결과
4. 개인정보보호 고려사항
5. 권고사항
6. 결론 및 정책적 시사점

1. 배경

- ▶ 기술 혁신을 통해 블록체인 기술을 기반으로 한 디지털 자산(Digital Assets)이 빠르게 확산되는 추세
 - 블록체인 기반의 디지털 자산은 전통적인 금융 상품을 넘어선 자산의 디지털 표상으로 금융 서비스를 변화시키고 있으며, 다양한 형태를 취하고 있음
 - 블록체인 기술은 국내외 자금 이체 및 결제 비용 절감 등에 기여하며 기존의 금융 서비스를 개선하고 확장할 뿐만 아니라, 불변성을 기반으로 예술 작품의 디지털 데이터 기록을 생성하는 등 여러 가지 새로운 기회를 제공

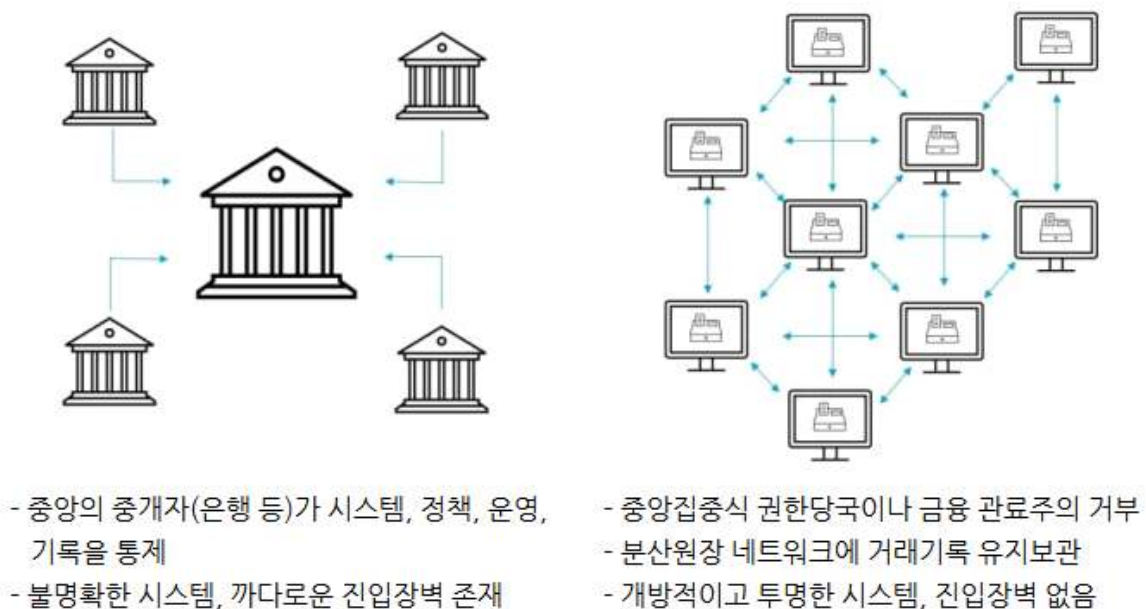
- 그러나 개방성을 특징으로 하는 블록체인 기술은 개인정보보호, 정보보안, 금융 안정성 등 여러 측면에 잠재적으로 중대한 영향을 초래
- ▶ 미국, 영국, 유럽연합(EU) 등 세계 각지의 금융기관들은 빠르게 발전하는 디지털 자산에 대한 합리적인 규제 방안을 모색 중
- 일관성 있으며, 포괄적이며, 실행 가능한 규제를 위해서는 금융 서비스 정책 및 규제 발전과 동시에 개인정보보호 이슈를 함께 고려하는 것이 중요
- 특히 개인정보보호가 디지털 자산의 신뢰성에 중대한 영향을 줄 수 있음을 고려할 때, 블록체인 생태계에는 개인정보보호와 금융 정책·규제 사이의 조화와 균형적인 상호작용이 필요
- ▶ 개인정보정책리더십센터(Centre for Information Policy Leadership¹³), 이하 CIPL)는 디지털 자산과 관련 규제가 발전하면서 부상한 주요 개인정보보호 과제 및 제반 사항들을 다양한 산업계 대표자 및 전문가들과 함께 심도 깊게 검토
- CIPL은 규제기관, 법률·정책 입안자, 산업계 지도자, 학계와 함께 디지털 자산이 개인정보보호에 끼치는 영향에 관한 공개회의 등을 개최하여 디지털 자산과 관련된 개인정보보호의 기회와 도전과제, 입법과 규제 도입 시 고려할 사항 등을 논의
- 특히 디지털 자산의 이용 및 개인정보보호와 관련하여 책임성, 보안성, 투명성, 정보주체 권리, 개인정보 국외 이전, 개인정보 최소화 등 주요 이슈들을 중점적으로 검토
- ▶ CIPL은 디지털 자산과 개인정보보호의 관련성을 주제로 CIPL 회원사들이 참여해 진행한 공개 토론회에서 얻은 통찰력을 종합하여 '23년 1월 20일 "디지털 자산 및 개인정보보호(Digital Assets and Privacy)"라는 제목의 토론문서를 발표
- 동 문서는 디지털 자산의 근간인 블록체인 기술에 초점을 맞춰 블록체인의 다양한 유형, 개인정보보호에 대한 영향, 입법·규제 개발의 맥락에서 일관되고 기술 친화적이며 미래 지향적이고 실용적인 접근을 위한 권장사항들을 제시
- 또한 디지털 자산의 신뢰성, 상호운용성 및 규제 일관성을 보장하기 위한 전 세계의 규제 기관 및 이해관계자들의 건설적인 대화와 참여를 촉구하면서, 일관적이고 포괄적이며 실행력 있는 규제를 위해 디지털 자산의 중첩된 규제 문제에 대한 연구가 필요함을 강조

13) CIPL은 미국 워싱턴 DC, 벨기에 브뤼셀 및 영국 런던에 기반을 둔 개인정보보호 및 관련 정책의 개발·실행을 위한 글로벌 싱크탱크로, 산업계 리더, 규제당국, 정책 입안자 등과 협력하여 개인정보보호 및 책임 있는 개인정보 사용을 위한 글로벌 솔루션 및 모범사례를 개발하는 데에 주력

2. 블록체인의 특성과 유형

- ▶ 블록체인 기술은 본질적으로 신뢰할 수 있는 중개자 없이 참여자가 탈중앙화된 네트워크 (일명 '노드')에서 거래 및 데이터를 기록하고 공유할 수 있도록 지원
- 블록체인은 제3의 중개자의 필요성을 없애고 데이터의 수집·저장·처리를 분산시킬 수 있는 기록 보관 기능을 제공하는데, 이러한 블록체인의 특성은 '중앙 집중화'를 특징으로 하는 현행 데이터 경제와 뚜렷한 대조를 이룸
- 일반적으로 각 블록체인 노드에는 최초로 생성된 블록에서 가장 최근에 생성된 블록까지 전체 원장의 완전한 사본이 저장됨
- 각 블록은 이전 블록, 타임스탬프(timestamp) 및 거래정보 등 관련 데이터를 포함

그림1 _ 중앙 집중식 금융 모델과 탈중앙화 금융 모델의 차이점

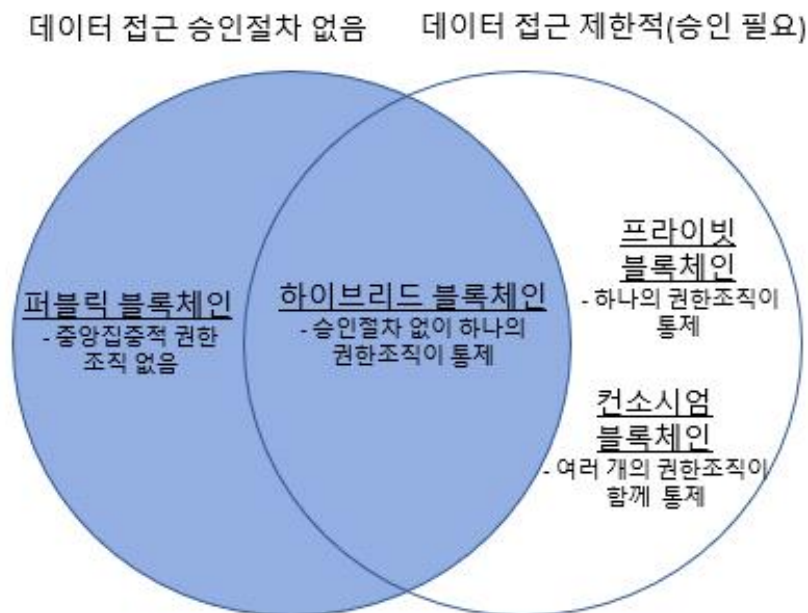


출처: CIPL, Digital Assets and Privacy, 2023.1

- ▶ 블록체인 네트워크의 주요 유형은 ▲퍼블릭(Public) 블록체인 ▲프라이빗(Private) 블록체인 ▲하이브리드(Hybrid) 블록체인 ▲컨소시엄(Consortium) 블록체인의 네 가지로 구분
- 퍼블릭 블록체인은 비(非)제한적이며, 데이터 접근에 대한 별도의 승인 없이 인터넷 이용이 가능한 사람이면 누구나 블록체인 주소를 생성하거나, 노드를 운영하거나, 채굴 활동이 가능
- 프라이빗 블록체인은 폐쇄된 네트워크와 같은 제한적인 환경에서 작동하거나 단일 권한 조직의 통제 하에 작동

- 하이브리드 블록체인은 프라이빗 및 퍼블릭 블록체인의 요소를 모두 포함하여, 권한을 가진 조직이 블록체인에 저장된 특정 데이터에 접근할 수 있는 사람과 공개적으로 사용할 수 있는 데이터를 제어
- 컨소시엄 블록체인은 프라이빗 및 퍼블릭 블록체인의 기능을 동시에 가지고 있다는 점에서 하이브리드 블록체인과 유사하나, 권한을 가진 다수의 조직 구성원들이 탈중앙화된 네트워크에서 협업한다는 점에서 하이브리드 블록체인과 구별
- * 예를 들자면 컨소시엄 블록체인에서는 여러 은행들이 함께 모여 컨소시엄을 구성하여 어떤 노드에서 거래를 승인할지 결정할 수 있음

그림2 _ 데이터 접근 승인 모델에 따른 주요 블록체인 유형 구분



출처: CIPL, Digital Assets and Privacy, 2023.1

3. CIPL 회의에서의 주요 논의 결과

- ▶ 금융 규제기관들은 정책·규제 분석과 개발의 초기 단계에서 개인정보보호 규제기관이 적극 참여하도록 함으로써, 개인정보보호에 대한 영향을 고려한 일관된 정책·규제를 개발할 수 있음
- 폐쇄적인 접근법을 통해 개발된 자금세탁방지(Anti Money Laundering) 규정은 여러 상충된 의무와 정책적 접근법들로 인하여 금융 테러를 예방하는 동시에 개인정보보호 의무를 준수해야 하는 산업계에 이미 여러 법적 불확실성을 유발 중

- ▶ 블록체인의 고유한 특성을 적절히 활용하면 기존의 문제점을 해결할 수 있음
 - 예를 들어, 투명성을 향상시키는 KYT(Know-Your-Transaction^{*}) 접근법은 금융 범죄에 대응하는 데에 블록체인의 속성을 활용할 수 있음을 보여줌
 - ^{*} 고객의 신원을 식별하고 확인하는(Verify) 업무절차로, 자금세탁을 포함하여 사기 또는 의심스러운 활동에 대한 금융 거래를 검사하는 프로세스
- ▶ 개인정보보호와 블록체인의 본질적인 특성 차이에서 발생하는 여러 상충된 문제들을 해결하기 위한 노력이 필요하며, 만약 이러한 현안들을 해결하지 못한다면 미래 기술 발전이 가로막힐 위험이 있음
 - 일반적으로 개인정보보호 규정은 개인정보에 대한 권한과 책임을 갖는 컨트롤러 또는 프로세서를 정의하고, 중앙집중식 권한 조직과 규제 준수 메커니즘을 바탕으로 개인정보보호를 다루도록 설계됨
 - 그러나 블록체인은 중앙집중식 권한 조직을 갖지 않으므로 개인정보보호 규정과 상충되는 특성을 보유
 - 따라서 기술적이고 창의적인 솔루션을 활용하여 블록체인과 개인정보보호 규정 사이의 여러 상충하는 문제들을 해결하고, 개인정보보호 체계를 조정해 성숙시킬 필요가 존재
 - 이를 위해서는 기존 개인정보보호의 개념과 정의를 재규정할 수 있는 개방성이 필요할 것이며, 또한 산업계 전반의 표준과 모범사례의 채택을 장려하는 새로운 규제 지침 등이 필요할 수 있음
- ▶ 디지털 자산 및 블록체인 기반 시스템은 개인정보보호 외에도 여러 중요한 이슈(테러 자금 조달 방지, 소비자 보호 등)들과 관련성이 있는데, 개인정보보호 우려는 그 무엇보다 우선적으로 검토되어야 함
 - 개인정보보호 규정 준수에 대한 명확성이 부재할 경우, 블록체인 정책에 대한 신뢰를 구축하기 어려움
 - 블록체인 정책에 대한 신뢰가 부족하면 블록체인을 기반으로 한 혁신 및 관련 사업 모델의 개발 및 도입에 지장 초래
- ▶ 성공적인 규제를 위해서는 달성 가능한 현실적인 목표 설정이 중요하며, 블록체인 기술 자체를 규제할 것인지 또는 블록체인 기반으로 작동하는 응용시스템을 규제할 것인지에 대한 판단이 필요함
- ▶ 블록체인에 대한 규제는 기술 중립적이면서, 위험에 기반 한(개인에게 미치는 위험 고려), 혼합방식(탈중앙 및 중앙집중 접근 방식 모두 활용)의 접근법이 필요하며, 블록체인에 대한 이용자의 기대치와 이해수준을 고려해야 함

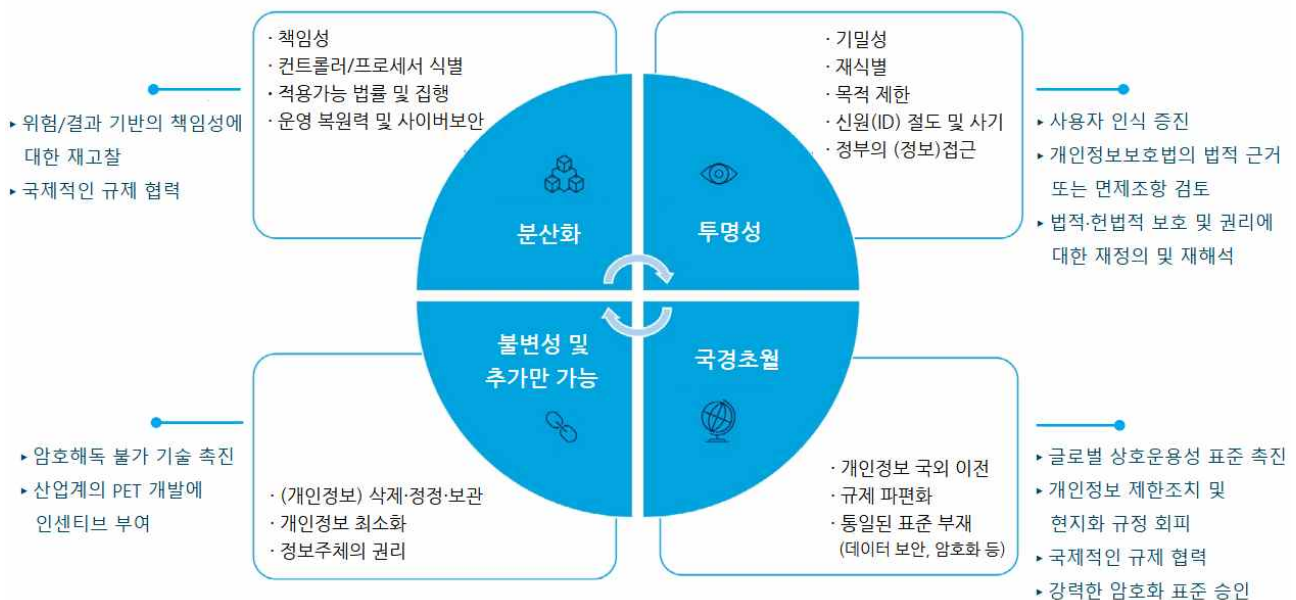
- ▶ 규제 기관은 블록체인을 성공 또는 실패라는 이분법적 사고방식으로 판단하기 보다는 블록체인의 기회와 위험을 인식하고 블록체인 기반의 디지털 자산에 대한 새로운 참여방식, 개념 적용, 규제 방안 등을 검토해야 함
- ▶ 블록체인은 국경을 초월해 활용되므로, 전 세계의 여러 규제 기관들이 블록체인 기반 애플리케이션을 통일성 있게 규제할 수 있도록 디지털 자산의 유형 분류 개발 등이 필요함
- ▶ 규제 당국은 개인정보보호 및 보안 관련 우려사항들을 다루는 데에 있어 블록체인의 탈중앙 생태계의 이점을 활용할 수 있는데, 특히 다음과 같은 블록체인의 특성들을 고려할 것이 권장됨
 - **(투명성)** 블록체인이 투명성은 불법 활동에 대한 가시성을 실시간으로 제공하므로, 적시에 처리해야 할 필수적인 개인정보의 양을 줄이면서 보다 개인정보 친화적인 접근 방식을 지원
 - **(추적성)** 대규모의 정보 수집이나 국제사법공조 요청 등과 같은 번거롭고 많은 시간이 소요되는 작업 없이도 신속하게 잘못된 점을 파악할 수 있도록 지원
 - **(공공성)** 보다 많은 정보가 공유되고, 전체 생태계가 악의적이거나 불법적인 활동을 공동으로 식별해 보고할 수 있도록 지원
 - **(영구성)** 악의적이거나 불법적인 활동을 블록체인의 전체 수명주기에서 더욱 쉽게 추적할 수 있도록 지원
 - **(프로그램 가능성)** 개인정보보호 강화기술(Privacy-enhancing technologies, 이하 PET) 및 혁신적인 도구를 활용할 수 있도록 지원(예, 디지털 여권, 디지털 지갑)

4. 개인정보보호 고려사항

- ▶ **(기존 법률 및 정의의 적용 가능성)** 블록체인 기술은 컨트롤러, 프로세서 등 현행 개인정보보호 규정에서 다루고 있는 기본 개념들과 상응하지 않고, 특정 관할권에 국한되지도 않으므로 기존의 개인정보보호 관련 정의 및 제도를 적용하기 어려움
- ▶ **(책임성)** 블록체인은 설계상 중앙에서 개인정보를 제어하지 않는 탈중앙화된 시스템이며, 이에 따라 개인정보 처리 수단과 목적을 결정하는 책임자에 대한 평가가 어려울 수 있음
- ▶ **(개인정보 최소화)** 블록체인 기술은 개별 블록에 개인정보를 저장하고, 이러한 블록들이 함께 연결되어 추가되면서 다양한 관할권의 여러 노드에서 영구적으로 저장되며 계속해서 팽창하는 데이터 네트워크를 생성

- ▶ **(목적 제한)** 블록체인의 고유한 특성으로 인해 블록체인에 저장된 개인정보 처리는 본래의 개인정보 처리목적에 부합하지 않을 수 있음
- ▶ **(개인정보 보안)** 이해관계자들이 적정 수준의 개인정보 보안을 위한 암호화 기술에 대해 합의하거나 표준화를 달성하지 못한 가운데, 블록체인의 투명성은 공개키를 표적으로 삼는 공격자들에게 취약점을 노출
- ▶ **(기밀성 및 정부 접근성)** 블록체인을 통해 정부를 포함한 모든 사람들은 더욱 투명한 방식으로 거래 확인이 가능
- ▶ **(정보주체의 권리)** 블록체인 거래는 삭제되지 않고 영원히 기록되며, 개인정보의 삭제·수정·이의제기·보존 등에 대한 정보주체의 권리 요청을 처리할 수 있는 단일 창구가 부재
- ▶ **(개인정보 국외 이전)** 국경을 초월하는 블록체인의 특성을 고려할 때 이해관계자들은 현행 개인정보 국외 이전 메커니즘의 적용 가능성을 검토하고, 현재와 미래의 개인정보 국외 이전에 대한 여러 대안들을 평가해야 함

그림3_ 블록체인 아키텍처에서 개인정보보호 관련 고려사항 및 시사점



출처: CIPL, Digital Assets and Privacy, 2023.1

5. 권고사항

- ① 관련 정책에서 블록체인과 개인정보보호 사이의 상호작용에 대해 다루고, 각종 규정, 지침, 양해 각서 및 기타 메커니즘을 통해 여러 이해관계자들을 안내

- ② 블록체인 기술의 특성 및 아키텍처와 일치하는 혁신적인 접근법(이상적으로는 기술 중립적이고 기능적이며 결과 중심적인 접근법)을 구현하고, 개인정보 전송 제한 및 개인정보 현지화 요구사항이 증가하면서 발생하는 문제를 해결
- ③ 정책과 규제가 산업계 주도로, 분야를 초월하여 조화롭게 적용될 수 있도록 개선
- ④ 혁신가 및 기타 이해관계자들과 소통하면서 사용자의 기대를 고려한 현실적이고 달성 가능한 목표 수립
- ⑤ 블록체인, 특히 퍼블릭 블록체인 네트워크에서 원하는 수준의 개인정보보호 권리 및 원칙을 달성할 수 있는 방법 마련
- ⑥ 블록체인과 관련한 개인정보보호 강화를 지원하기 위하여 영지식 증명(零知識證明)* 등 산업계에서 인정한 표준 및 샌드박스 활용 장려

* Zero-Knowledge Proof: 개인(prover)이 자신만이 보유한 비밀 정보를 공개하지 않고 상대방인 확인자(verifier)에게 정보를 알고 있음을 증명할 수 있는 암호화 체계
- ⑦ 퍼블릭 블록체인에서 개인정보보호와 투명성 사이의 긴장으로 인해 발생하는 법, 규제, 헌법과 기본권 측면에서의 영향을 이해관계자와 함께 검토하고, 기술적 조치와 모범사례 탐색
- ⑧ 기존의 집행 조치가 블록체인 환경에서도 효과적이고 적절하도록 개선방안 검토
- ⑨ 금융 서비스 당국, 경쟁당국, 개인정보보호 당국 등 여러 규제기관들의 개인정보 관련 협력과 협업 보장
- ⑩ 다양한 분산원장 솔루션 간 개인정보 이동성과 글로벌 상호운용성을 달성하기 위한 혁신 촉진
- ⑪ 산업계로 하여금 쉽게 접근할 수 있고 확장성이 있으며 블록체인의 특성에 적합한 암호화 및 기타 보안조치에 대한 강력한 표준을 수립할 수 있는 수단과 기법을 탐색하도록 유인책 부여
- ⑫ 산업계가 디지털 지갑 보유자의 무결성과 저장된 개인 키의 보안을 보장하는 안전한 기술 인프라를 개발하도록 장려
- ⑬ 퍼블릭 블록체인에서 책임성을 보장하기 위한 대안적 접근방식 검토
- ⑭ 개인 키 관련 위험, 피싱 공격, 기존 물리적 보안의 이점 등 블록체인 생태계와 관련된 위험에 대한 사용자 교육 실시
- ⑮ 블록체인 데이터에 대한 정부의 접근과 관련하여 정부의 투명성을 지속 개선하고 강력한 프로세스와 보호 장치를 구현

6. 결론 및 정책적 시사점

- ▶ 규제 기관들은 혁신을 저해할 수 있는 규칙을 성급히 도입하기 전에 개인정보보호와 블록체인의 상충되는 속성에 기인한 긴장을 조정할 필요가 있음
 - 블록체인 기술 사례가 아직 완전히 개발되지 않은 상황에서 과도한 규제를 적용할 경우 블록체인 기술 활성화를 저해할 위험이 존재
 - 다만, 블록체인 기반 시스템에서 컨트롤러에 대한 규제를 명확히 정의한다면 블록체인 생태계는 개인정보보호를 지원하면서 번영하고 발전할 수 있음
- ▶ 데이터 난독화(Data Obfuscation*), 해싱(Hashing), 암호화 등과 같은 기술을 활용하여 블록체인에서 기존의 개인정보보호 원칙들을 수호하는 것에 초점을 맞추는 것이 중요
 - * 소프트웨어나 권한이 있는 사람이 계속 사용할 수 있으면서도 권한이 없는 침입자에게는 가치가 없거나 거의 없는 방식으로 중요한 데이터를 수정하는 프로세스
 - 이와 동시에 명확하고 투명한 사용자 정보와 위험 인식을 기반으로 국경을 초월한 조화로운 국제 산업 표준 및 모범사례 개발에 대한 노력이 필요
- ▶ 국경을 초월하는 블록체인의 특성에 대한 명확한 인식을 통해 정책·규제 관련 국내외 협력과 상호인식을 발전시킬 수 있으며, 규제 관할권 충돌 및 불일치 문제도 해결할 수 있음
- ▶ 개인정보보호 권리는 다른 모든 권리에 우선하는 절대적인 권리가 아니며, 다른 법률에서 정의하는 기본적인 권리와 균형과 조화가 필요
 - 개인정보보호에 대한 권리는 사회적인 기능 측면에서 검토되어야 하며, 다른 기본권과 적절한 균형이 필요
 - 또한 금융 및 자금세탁 방지 규정을 포함한 다른 규정과 조화를 이루어야 함

Reference

1. CIPL, Digital Assets and Privacy, 2023.1
2. Hunton Andrews Kurth(Blog), CIPL Publishes Discussion Paper on Digital Assets and Privacy, 2023.1.20

〈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

2023

개인정보보호 월간동향분석 제1호

발 행 2023년 3월 3일

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

1. 본 보고서는 개인정보보호위원회 출연금으로 수행한 사업의 결과입니다.
2. 본 보고서의 내용을 발표할 때에는 반드시 한국인터넷진흥원 사업의 결과임을 밝혀야 합니다.
3. 본 보고서의 판권은 한국인터넷진흥원이 소유하고 있으며, 허가 없이 무단전재 및 복사를 금합니다.

※ 본 보고서의 내용은 한국인터넷진흥원의 공식 입장과는 다를 수 있습니다.