미국의 캘리포니아주 소비자 프라이버시법상 주요 내용 및 시사점

이창범 | 연세대학교 법학전문대학원 겸임교수

Ⅰ. 들어가는 글

2018년 6월 28일 제정된 「캘리포니아주 소비자 프라이버시법(California Consumer Privacy Act: CCPA)」은 캘리포니아주 「민법전(Civil Code)」 제1.81.5편[1]에 편제되어 있으며 소비자의 개인정보 권리와 사업자의 개인정보보호 의무를 규율하고 있는 법률로써 미국 역사상 가장 강력하고 고비용적인 개인정보보호법으로 평가받고 있다. 특히 미국에서의 온라인 광고환경에 지대한 영향을 미칠 것으로 예상된다.[2]

「캘리포니아주 소비자 프라이버시법(CCPA)」는 전통적으로 일반법(umbrella system)보다는 개별법(patchwork system)을 더 선호하는 미국의 전통과 달리 전 산업에 걸쳐 적용되는 일반법 성격의 개인정보보호법이라는 점에서 의의가 있다[3]. 또한 동법은 미국이나 캘리포니아주에서 설립된 사업자가 아니라도 캘리포니아주 소비자(주민)의 개인정보를 처리하는 역외의 사업자들에게도 적용된다는 점에서 국내 기업에 미치는 영향이 유럽연합의 「일반개인정보보호규정(General Data Protection Regulation: GDPR)」 못지 않게 클 수 있다.

1 §1798.100부터 §1798.199까지 총 19개 조문으로 구성되어 있다.

2 캘리포니아주의 개인정보 프라이버시 법 제정에 기여한 억만장자의 최상류 부유층은 앞으로도 광고 산업을 규제하고 빅 테크(big tech) 로비스트와 투쟁할 것을 밝힌바 있다. "The billionaire behind California's sweeping new data privacy law reveals his plans to further regulate the ad industry and fight big tech lobbyists."

3 「캘리포니아주 소비자 프라이버시법(CCPA)」는 주 전체에 적용되며, 사업자에 의한 소비자의 개인정보 수집 및 판매와 관련하여 시, 군, 읍, 그 밖의 지방정부기관에 의해서 채택된 모든 규칙, 규정, 명령, 조례 및 그 밖의 법령을 대체하고 우선해서 적용된다(§1798.180).

「캘리포니아주 소비자 프라이버시법(CCPA)」는 개인정보처리 활동의 투명성(transparency) 강화와 함께 개인정보 처리에 대한 정보주체의 통제권(control) 및 사업자의 책임성(accountability) 강화를 기본 철학으로 하고 있다는 점에서[4] 유럽연합의 「일반개인정보보호규정(GDPR)」과 입법 목적이 유사하다. 개인정보의 정의, 가명 및 익명 정보의 활용, 정보주체의 권리 보호, 사업자의 고지·공개 의무 등도 「일반개인정보보호규정(GDPR)」의 영향을 받은 것이라고 할 수 있다.

이처럼 「캘리포니아주 소비자 프라이버시법(CCPA)」는 「일반개인정보보호규정(GDPR)」의 영향을 많이 받아 유사한 내용이 적지 않지만, 「일반개인정보보호규정(GDPR)」과 달리 개인정보처리 제한권, 자동의사결정 거부권, 이용 및 보유 기간의 제한, 처리 활동의 기록·관리, 기술적·관리적 조치, 프라이버시 영향평가, 개인정보보호책임자(Data Protection Officer: DPO) 및 대리인 지정, 개인정보 국외이전 등에 대해서는 규정을 두고 있지 않거나 부분적으로만 규정하고 있다. 반면, 「캘리포니아주 소비자 프라이버시법(CCPA)」는 「일반개인정보보호규정(GDPR)」에는 없는 고유의 독창적인 권리·의무 규정을 적지 않게 하고 있다.

즉, 개인정보 판매 중단 지시(Do-Not-Sell) 링크 설정, 권리행사를 이유로 정보주체에 대한 차별대우 금지 등과 같은 특유의 의무규정을 두고 있고, 법 위반시 고액의 민사벌금은 물론 소비자 단체소송(class action), 법정손해배상청구, 금지명령, 확인의 소 등 다양한 제재 및 권리구제 수단을 마련해 두고 있다. 또한, 「캘리포니아주 소비자 프라이버시법(CCPA)」는 캘리포니아주 밖에서 설립된 사업자에게도 적용될 수 있다.

공식적으로 「캘리포니아주 소비자 프라이버시법(CCPA)」는 2020년 1월 1일부터 시행되나(§1798.198 (a)), 동법에 따라 사업자가 준수해야 할 정보공개, 정보이전 등의 의무는 법·시행 전 과거 12개월 동안 처리된 개인정보도 공개, 이전 등의 대상이 되므로 사실상 「캘리포니아주 소비자 프라이버시법(CCPA)」는 2019년 1월 1일부터 시행되고 있다고 볼 수 있다. 이에 따라 대다수 미국의 IT기업들은 2019년 1월부터 개인정보의 수집출처, 수집·판매하는 개인정보 항목, 제3자의 범주 등을 조사·정리하면서 사실상 「캘리포니아주 소비자 프라이버시법(CCPA)」 이행 준비에 들어간 상태이다.[5] 다만, 하위법령의 제정 지연으로 주 법무장관은 2020년 6월 30일까지 이 법을 집행하지 못한다(§1798.185 (a)·(c)).[6]

4 Testimony of Alastair Mactaggart, United States Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, Wednesday, October 10th, 2018

5 California Consumer Privacy Act (CCPA): What you need to know to be compliants.

6 주 법무장관은 2020년 7월 1일까지 「캘리포니아주 소비자 프라이버시법(CCPA)」 시행규칙을 채택해야 하나(§1798.185 (a)), 현재 규칙 초안에 대해서 주민의견을 수렴 중이다. 주 법무장관은 이 조항에 의해 제정된 최종 시행규칙이 공포된 이후 6개월 또는 2020년 7월 1일 중에서 보다 이른 때까지 이 법에 따라 시행 조치를 취하지 않는다(§1798.185 (c)).

「캘리포니아주 소비자 프라이버시법(CCPA)」는 2019년 5월에 이어 10월에도 대폭적인 개정이 있었다. 이하에서는 개정법을 중심으로 개인정보보호법의 핵심 이슈인 개인정보의 정의, 적용범위, 정보주체의 권리, 사업자의 의무, 벌칙 및 권리구제 등을 중심으로 「캘리포니아주 소비자 프라이버시법(CCPA)」의 주요 특징과 시사점을 분석하기로 한다.

Ⅱ. 「캘리포니아주 소비자 프라이버시법(CCPA)」의 적용 대상 및 범위

1. 소비자의 범위

「캘리포니아주 소비자 프라이버시법(CCPA)」의 보호대상은 소비자이다. '소비자(consumer)'란 캘리포니아주 주민인 자연인으로서 고유식별자(unique identifier) 등에 의해서 식별되는 자를 의미한다(§1798.140(g)).[7] 「캘리포니아주 규정집(California Code of Regulations)」 제18장 제17014조는 '주민(resident)'을 (1) 임시적 또는 일시적 목적 이외의 목적으로 캘리포니아주에 있는 모든 개인과 (2) 캘리포니아주에서 거주하지만 임시적 또는 일시적 목적으로 캘리포니아주 밖에 있는 모든 개인을 포함한다고 규정하고 있다.

이에 따르면 주민에는 소비자뿐만 아니라 근로자도 포함된다.[8] 즉, 물품이나 서비스를 구입하는 구매자 이외에 근로자, 협력업체 또는 공급업체 임직원, 개인사업자 등도 소비자에 포함될 수 있다. 또한, 「캘리포니아주 소비자 프라이버시법(CCPA)」는 캘리포니아주 밖을 여행 중에 있는 캘리포니아주 주민의 소유에 속하는 모바일 기기의 웹사이트 브라우징 내역이나 위치정보의 처리에 대해서도 적용된다.

7 원문의 내용은 다음과 같다.: 'Consumer' means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

8 What is a 'consumer' under the CCPA? Dec 1, 2018.

그러나 2019년 법 개정으로 해당 사업자의 구직자, 근로자, 소유자, 이사(director), 임원(officer), 의료진, 계약자(contractor)가 현재 또는 과거에 자신의 역할 수행 과정에서 사업자에 의해서 수집·이용된 개인정보, 비상연락망, 연금·지원금 정보에 대해서는 2021년 1월 1일까지 한시적으로 「캘리포니아주 소비자 프라이버시법(CCPA)」의 적용이 면제된다(§1798.145 (h). 이와 같은 면제를 근로자 적용면제(employee exemption)라 한다. 다만, 개인정보 열람권 및 이동권(§1798.100)과 권리구제(§1798.150)에 관한 조항은 적용이 면제되지 않으므로 사업자는 개인정보의 수집 시점 또는 그 이전에 수집할 개인정보의 범주와 개인정보의 이용 목적을 소비자에게 알려야 하고, 개인정보 열람권 및 이동권을 준수해야 하며, 소비자는 개인정보 보호조치 의무 위반을 이유로 민사소송을 제기할 수 있다.

또한 사업자가 기업간(Business-To- Business, 이하 B2B) 관계에서 다른 회사, 파트너십, 개인회사, 비영리기관, 정부기관의 근로자, 소유자, 이사, 임원, 계약자와 업무상 소통 또는 거래 과정에서 사업자가 상당한 주의를 가지고 수집한 개인정보에 대해서는 2021년 1월 1일까지 한시적으로 개인정보 열람권 및 이동권(§1798.100), 삭제요구권(§1798.105), 정보공개요구권(§1798.110, §1798.115), 권리의 행사 및 이행 방법(§1798.130), 개인정보 판매 공개의무(§1798.135)에 관한 조항은 적용이 면제된다(§1798.145 (n)). 이와 같은 면제를 사업자간 거래면제(B2B exemption)라 한다. 다만, 개인정보 판매 중단 지시권, 소비자 차별금지 의무, 권리구제 및 벌칙규정 등은 면제되지 않는다.

2. 사업자의 범위

「캘리포니아주 소비자 프라이버시법(CCPA)」의 준수주체는 사업자이다. '사업자(business)'란 캘리포니아주에서 영리를 목적으로 사업을 경영하는 자로서 캘리포니아주 주민의 개인정보를 직접 수집하거나 다른 사업자를 통해서 수집하고 단독으로 또는 다른 사업자와 공동으로 개인정보 처리의 목적과 방법을 결정하는 개인사업자, 조합(파트너십), 유한회사, 주식회사, 협회, 그 밖의 법적 실체를 의미한다(§1798.140 (c)). 영리 목적이 있어야 하므로 주 및 지방 정부, 비영리 단체 등에 대해서는 적용되지 않는다.

그러나 모든 사업자에게 「캘리포니아주 소비자 프라이버시법(CCPA)」가 적용되는 것은 아니다. 연간 총 매출액이 2천5백만 달러 이상이거나, 상업적 목적으로 연간 5만 명/개 이상의 캘리포니아주 소비자·가계·기기에

관한 개인정보를 단독으로 또는 결합해서 구입, 수령, 판매 또는 공유하거나, 연간 매출액의 50% 이상이 캘리포니아주 소비자의 개인정보 판매로 발생한 자에 대해서만 적용된다(§1798.140 (c)(1) (A)·(B)·(C)).[9] 그러나 연간 매출액이나 소비자·가계·기기의 수를 산정할 때 캘리포니아주를 기준으로 해야 할지 전 세계를 대상으로 해야 할지는 분명하지 않다. 일부 전문가들은 전 세계 매출로 보아야 한다는 의견을 제시하고 있다.[10]

또한 「캘리포니아주 소비자 프라이버시법(CCPA)」는 해당 사업자(캘리포니아주 주민의 개인정보를 처리하는 자)와 공동 브랜딩(common branding)[11]을 공유하는 모회사 및 자회사에게도 적용된다. 즉, 해당 사업자를 지배하거나(모회사) 해당 사업자에 의해서 지배를 받으면서(자회사) 공동으로 브랜드를 공유하는 사업자에게도 적용된다(§1798.140 (c)(2)). 따라서 공동 브랜드를 이용하고 있는 해당 조직 그 자신은 「캘리포니아주 소비자 프라이버시법(CCPA)」 하에서 사업자에 해당하지 않더라도 사업자의 지배를 받고 있거나 사업자를 지배하고 있는 자에 대해서는 이 법이 적용된다.[12]

다만, 모든 상업적 활동이 전적으로 캘리포니아주 밖에서 이루어지는 사업자에게는 「캘리포니아주 소비자 프라이버시법(CCPA)」가 적용되지 않는다(§1798.145 (a)(6)). 예컨대, 소비자가 캘리포니아주 밖에 있는 동안 개인정보를 수집하였고, 해당 개인정보의 판매 활동 중 일부라도 캘리포니아주 내에서 이루어지지 않았으며, 소비자가 캘리포니아주에 있는 동안 수집된 개인정보가 전혀 판매되지 않았다면 「캘리포니아주 소비자 프라이버시법(CCPA)」는 적용되지 않는다.

9 이에 따라 회사의 규모가 크지 않은 실리콘 밸리의 소규모 사업자들에게는 「캘리포니아주 소비자 프라이버시법(CCPA)」의 적용이 면제된다.

10 "Are You Prepared for the California Consumer Privacy Act? Get Ready for European-Style Privacy in the U.S."

11 상호, 서비스마크, 트레이드마크(상표) 등을 공동으로 이용하는 것을 말한다. 다만, 이 경우 모회사는 자회사에 대하여 50% 이상의 소유권 또는 의결권을 가지고 있어야 한다.

12 California Consumer Privacy Act FAQs for Covered Businesses.

3. 지리적 적용 범위

「캘리포니아주 소비자 프라이버시법(CCPA)」는 역외 사업자에 대한 적용에 관해서 명확한 규정을 두고 있지 않으나, 온라인 환경에서 확립된 "doing business"이론에 따라 캘리포니아주에 있는 소비자 또는 근로자의 개인정보를 처리하는 역외의 사업자에게도 적용되는 것으로 해석되고 있다.[13] 따라서 사업자의 국적은 문제가 되지 않는다. 영리를 목적으로 캘리포니아주에서 사업을 수행하고, 캘리포니아주 소비자의 개인정보를 수집하며, 개인정보를 처리하는 목적과 방법을 결정하는 사업자에게는 「캘리포니아주 소비자 프라이버시법(CCPA)」가 적용된다. 캘리포니아주에 주소를 두지 않아도 되고, 미국에 주소를 두지 않아도 되며, 캘리포니아주나 미국에 물리적 실체가 존재하지 않아도 된다.

해당 사업자가 지리적으로 캘리포니아주에 존재하지 않아도 캘리포니아주 주민의 개인정보를 수집하거나 판매하는 사업자라면 「캘리포니아주 소비자 프라이버시법(CCPA)」가 적용된다. 예컨대, 캘리포니아주 소비자가 캘리포니아주 밖에 있는 식당을 방문한 경우에는 「캘리포니아주 소비자 프라이버시법(CCPA)」가 적용되지 않으나, 캘리포니아주 소비자가 캘리포니아주에서 있는 동안 캘리포니아주 밖에 있는 식당을 예약한 경우에는 「캘리포니아주 소비자 프라이버시법(CCPA)」가 적용된다. 그 밖에 캘리포니아주에 어떤 연결점(nexus)이 있는 사업자로서 캘리포니아주 주민의 개인정보를 처리하는 사업자에게도 「캘리포니아주 소비자 프라이버시법(CCPA)」는 적용된다.

4. 산업적 적용 범위

「캘리포니아주 소비자 프라이버시법(CCPA)」는 미국 최초의 개인정보보호 일반법으로서 원칙적으로 공공부문을 제외한 모든 산업에 적용된다. 다만, 연방 데이터 보호법에 의하여 보호를 받고 있는 산업에 대해서는 「캘리포니아주 소비자 프라이버시법(CCPA)」가 적용되지 않는다(§1798.145 (c)).

대표적으로 건강보험법(HIPAA), 의료정보보호법(CMIA) 등의 적용을 받고 있는 보건서비스 제공자 및 보험회사, 금융현대화법(Gramm-Leach-Bliley) 등의 적용을 받고 있는 은행 및 금융회사, 「공정신용보고

13 "California Consumer Privacy Act (CCPA): What you need to know to be compliants".

법(Fair Credit Reporting Act)」의 적용을 받고 있는 신용보고기관, 「운전자 프라이버시 보호법(Driver's Privacy Protection Act)」에 따른 운전자 정보 등은 「캘리포니아주 소비자 프라이버시법(CCPA)」의 적용 범위에서 제외된다.

5. 개인정보의 범위

개인정보란 직·간접적으로 특정 소비자 또는 가계를 식별(identifies)하거나, 설명(describes)하거나, 특정 소비자 또는 가계와 관련(relate)되거나, 합리적으로 연관(associate)시킬 수 있거나, 합리적으로 연결(link)시킬 수 있는 정보를 의미한다(§1798.140 (o)(1)). 개인정보는 전자적 또는 인터넷을 통해서 수집되는 정보에 한정되지 않고 사업자가 소비자로부터 수집한 모든 개인정보의 수집 및 판매에 적용된다(§1798.175). 이름, 사회보장정보 등 전통적인 형태의 개인식별정보뿐만 아니라 기기식별자, 행태정보, 바이오정보, 추론정보 등도 포함된다. 구체적으로 아래의 정보가 포함되나, 이에 한정되지 않는다.

(1) 식별자(Identifiers) : 실명, 가명(가명), 우편주소, 고유식별자[14], 온라인 식별자, 인터넷 프로토콜(IP) 주소, 전자우편 주소, 계정 이름, 사회보장번호, 운전면허번호, 여권번호, 그 밖에 이와 유사한 식별자

(2) 「캘리포니아주 민법전(Civil Code)」 §1798.80 (e)에 의해서 보호받고 있는 개인정보[15]

(3) 캘리포니아주법 또는 연방법에 의해 보호를 받는 특정 부류의 특성에 관한 정보[16]

(4) 상업적 정보(commercial information) : 개인의 재산 내역, 구매하거나 취득하거나 관심을 보인 물품 또는 서비스 목록, 구매 또는 소비 내역이나 성향 등

14 '고유 식별자'란 시간이 흐름에도 불구하고 다양한 서비스에 걸쳐서 소비자, 가족, 소비자 또는 가족과 연결되어 있는 단말기를 인식하는 데 사용할 수 있는 영구 식별자를 의미한다(§1798.140 (x)). 이에는 단말기 식별자, 인터넷 프로토콜 주소, 쿠키·비콘·픽셀 태그·모바일 광고 식별자 그 밖에 이에 유사한 기술, 고객 번호, 고유한 가명 또는 이용자 별명(닉네임), 특정 소비자 또는 단말기를 식별하는데 사용할 수 있는 전화번호, 그 밖의 형태의 영구적 또는 확률적 식별자 등이 포함되지만, 이에 한정되지 않는다. 이 경우 '확률적 식별자(probabilistic identifiers)'란 개인정보의 정의에 열거된 범주에 포함되거나 이와 유사한 범주의 개인정보 범주에 기초하지 않고는 개연성의 정도를 가지고 소비자 또는 단말기를 식별하는 것을 의미한다(§1798.140 (p)).

15 특정 개인의 이름, 서명, 사회보장번호, 신체적 특징 또는 설명, 주소, 전화번호, 여권번호, 운전면허번호, 캘리포니아주 주민카드 번호, 보험 증권번호, 교육, 고용, 고용경력, 은행계좌번호, 신용카드번호, 직불카드번호, 기타 금융정보, 의료정보, 건강보험 정보 등. 다만, 연방, 주, 지방 정부기록으로부터 일반인이라면 누구든지 적법하게 이용할 수 있는 정보로써 공개적으로 이용 가능한 정보는 제외한다.

16 인종, 피부색, 종교 또는 신념, 국적 또는 선조(조상), 성별, 연령, 신체적 또는 정신적 장애, 임신, 가족 상태, 재향 군인 자격, 유전 정보, 시민권 등 주로 고용차별과 관련된 정보들이다.

(5) 바이오정보(생체정보)[17]

(6) 인터넷 그밖의 전자네트워크 활동 정보 : 브라우징(인터넷 사용) 기록, 검색 기록, 인터넷 웹사이트·애플리케이션·광고에 대한 소비자의 반응(interaction) 등

(7) 지리적 위치정보(geolocation data)

(8) 청각(음향) 정보, 전자정보, 시각정보, 열(온도)정보, 후각정보, 그밖에 이에 유사한 정보

(9) 직업 또는 고용과 관련된 정보

(10) 교육정보 : 가족 교육의 권리 및 사생활 보호법(20 U.S.C. Sec. 1232g; 34 C.F.R. 99)에서 규정하고 있는 공개적으로 이용 가능한 개인식별정보는 제외

(11) 추론(inferences) : 특정 소비자의 선호, 특성, 심리적 성향, 성질(소인), 행동, 태도, 지능, 능력, 적성(소질) 등을 반영하는 소비자의 프로파일을 생성하기 위해 (1)~(10)까지의 정보로부터 도출된 추론

「캘리포니아주 소비자 프라이버시법(CCPA)」의 개인정보 정의는 기존의 여러 캘리포니아주 법률에서 사용 중인 개인정보의 개념보다 넓으며, 「일반개인정보보호규정(GDPR)」의 개인정보 정의와 유사하나 가계(a household)에 관한 정보가 포함된다는 점에서 특징적이라고 할 수 있다. 다만, 「일반개인정보보호규정(GDPR)」과 달리 공개적으로 이용이 가능한 정보는 개인정보로 보지 아니한다(§1798.140 (o)(2)). "공개적으로 이용 가능한 정보"란 연방, 주, 지방 정부의 기록에서 합법적으로 이용이 가능한 정보를 의미한다. 주의할 것은 연방, 주 또는 지방 정부기록에서 직접 수집한 정보만 「캘리포니아주 소비자 프라이버시법(CCPA)」 적용이 제외되고 제3자로부터 간접적으로 수집한 정보에 대해서는 「캘리포니아주 소비자 프라이버시법(CCPA)」의 적용이 면제되지 않는다.

또한 비식별 조치된 소비자 정보 및 총계화된 소비자 정보도 개인정보로 보지 아니한다(§1798.140 (o)(3)). 당초 「캘리포니아주 소비자 프라이버시법(CCPA)」에서는 이 부분이 불분명했으나 2019년 10월 법 개정으로 이를 명확히 했다. "비식별 조치된 소비자 정보(de-identified personal data)"란 특정 소비자 또는 가계를 합

17 개인의 데옥시 리보 핵산(DNA)을 포함한 개인의 생리적, 생물학적 또는 행동적 특성을 의미한다. 바이오정보는 단독으로 또는 서로 결합하여 또는 다른 식별 데이터와 함께 이용되어 개인의 정체성을 확립할 수 있다(§1798.140 (b)). 주로 홍채, 망막, 지문, 얼굴, 손, 손바닥, 정맥패턴, 음성녹음 등의 이미지를 포함하지만, 이에 국한되지는 않는다. 바이오정보로부터 얼굴윤곽, 성문 등과 같은 식별자 템플릿, 키 스트로크 패턴, 보행 패턴, 식별정보를 포함한 수면·건강·운동 데이터를 추출 할 수 있다.

리적으로 식별할 수 없거나, 관련지울 수 없거나, 설명할 수 없거나, 직·간접적으로 결합 또는 링크할 수 없는 정보를 의미한다. 이 경우 비식별 정보를 이용하는 사업자는 소비자의 재식별을 금지하는 기술적 보호 조치를 시행하고, 재식별을 구체적으로 금지하는 비즈니스 프로세스와 비식별정보의 부주의한(우발적인) 공개를 방지하기 위한 비즈니스 프로세스를 구현해야 하며, 재식별하려고 하는 시도를 금지해야 한다(§1798.140 (h)). "총계화된 소비자 정보"(aggregated consumer information)란 개별 소비자의 신원이 제거되어 어떤 소비자 또는 가계와도 연결되어 있지 않거나 합리적으로 연결할 수 없는 특정 소비자의 그룹 또는 범주와 관련한 정보를 의미한다(§1798.140 (a)).

Ⅲ. 소비자의 권리

「캘리포니아주 소비자 프라이버시법(CCPA)」는 소비자에게 자신에 관한 개인정보를 통제할 수 있는 다양한 권리를 부여하고 있다. 「캘리포니아주 소비자 프라이버시법(CCPA)」가 인정하고 있는 소비자의 권리로는 개인정보 열람권 및 이동권(§1798.100), 정보공개 요구권(§1798.110, §1798.115), 삭제 요구권(§1798.105), 판매중단 지시권(§1798.120) 등이 있다. 유럽연합 「일반개인정보보호규정(GDPR)」이 명시적으로 규정하고 있는 동의권, 정정요구권, 처리제한권, 처리반대권, 자동화된 의사결정 거부권 등의 권리는 인정하지 않거나 부분적으로만 인정하고 있다.

1. 개인정보 열람권 및 이동권

소비자는 사업자가 수집한 "개인정보의 범주와 항목"에 대해서 공개할 것을 요구할 권리를 가진다(1798.100 (a)). 사업자는 요구가 정당한 권한을 가진 자에 의한 것임을 확인한 후 소비자에게 개인정보를 제공해야 한다(1798.100 (c)). 요구받은 개인정보는 문서로 제공해야 하고, 소비자의 선택에 따라 일반우편이나 전자적 방식으로 전달해야 한다. 전자적으로 제공할 때에는 휴대 가능해야 하고 소비자가 방해받지 않고 개인정보를 다른 사업자에게 전송할 수 있도록 기술적으로 읽기 쉬운 형식이어야 한다. 개인정보는 무료로 제공되어야 하지만, 사업자는 12개월 동안 2회 이상 제공할 의무는 없다(§1798.100 (d), §1798.130 (a)(2)).

「캘리포니아주 소비자 프라이버시법(CCPA)」의 정보이동권이 「일반개인정보보호규정(GDPR)」의 그것과 다른 점은 소비자가 자신의 개인정보를 자신이 지정한 다른 사업자에게 이전해달라고 요구할 권리가 없다는 점과 개인정보 열람·이동 의무가 최근 12개월 내에 처리된 것으로 한정된다는 점이다. 또한 정보이동권의 대상이 되는 정보가 정보주체의 동의에 의해서 수집된 개인정보와 계약 체결 또는 이행을 위해 수집된 개인정보에 한정되지 않고, 자동화 수단에 의하여 처리되는 개인정보일 것도 요구하지 않는다. 사업자가 분석·가공해서 생산한 개인정보까지 열람권 및 이동권의 대상이 될지 여부는 분명하지 않다.

2. 정보공개 요구권

소비자는 사업자에게 수집 또는 판매한 자신의 개인정보에 대한 정보의 제공을 요구할 수 있다. 사업자는 요구가 정당한 권한을 가진 자에 의한 것임을 확인 가능한 경우에는 소비자에게 최근 12개월 내에 수집하거나 판매·제공한 아래의 정보를 무료로 제공해야 한다(1798.110 (a)·(b), 1798.115 (a)·(b)).

소비자가 요구할 수 있는 정보는 수집·이용의 경우와 판매·제공의 경우에 차이가 있다. 소비자가 개인정보를 수집·이용한 사업자에 대해서 요구할 수 있는 정보는 아래와 같다(1798.110 (a)·(b)).

(1) 소비자에 관해 수집한 개인정보의 범주

(2) 개인정보를 수집한 출처의 범주

(3) 개인정보의 수집 또는 판매를 위한 사업(업무) 또는 상업 목적[18]

18 「캘리포니아주 소비자 프라이버시법(CCPA)」는 개인정보의 이용 목적을 '사업 목적'과 '상업 목적'으로 엄격히 분리하고 차별적인 의무를 부여하고 있다. '사업 목적'이란 사업체의 운영 목적 또는 개인정보가 수집된 상황과 양립 가능한 다른 운영상의 목적을 달성하기 위해 합리적으로 필요하고 비례적인 범위 내에서, 사업자 또는 수탁자가 개인정보를 이용하는 것을 의미한다. 사업 목적에는 다음과 같은 것이 포함된다(§1798.140 (d)) : (1) 소비자와 실시간 상호작용 및 동시거래에 대한 감사 : 특정 방문자에 대한 광고 노출 횟수 계산, 광고 노출의 장소 및 품질 확인, 설명서 및 기타 표준의 준수 여부에 대한 감사를 포함하되 이에 국한하지 아니한다. (2) 보안사고 탐지, 악의적·기만적·사기적·불법적인 활동으로부터의 보호, 그와 같은 활동에 대하여 책임이 있는 자에 대한 기소. (3) 기존의 의도된 기능을 손상시키는 오류를 식별하고 복구하기 위한 디버깅. (4) 단기간의 일시적인 개인정보 이용. 다만 개인정보가 다른 제3자에게 공개(제공)되지 않아야 하고, 소비자에 관한 프로파일을 작성하거나 실시간 상호작용 밖에서 개인 소비자의 경험을 변경하는데 사용되지 않아야 한다. 동일한 상호작용의 일부로 표시된 상황별 맞춤 광고를 포함하되 이에 국한하지 아니한다. (5) 사업자 또는 수탁자를 대신한 서비스의 이행 : 계정의 유지·점검, 고객 서비스 제공, 주문 및 거래의 처리 또는 이행, 고객정보 확인, 지불 처리, 금융 제공, 광고 또는 마케팅 서비스의 제공, 분석 서비스 제공, 사업자 또는 서비스 제공자를 대신한 유사 서비스의 제공. (6) 기술 개발 및 실증을 위한 내부 연구의 착수. (7) 사업자가 소유, 제조, 통제하거나 사업자를 위해 제조된 서비스 또는 단말기의 품질 또는 안전성을 확인 또는 관리하기 위한 활동 및 개선·업그레이드·향상시키기 위한 활동. 반면, (f) '상업적 목적'이란 다른 사람이 제품, 상품, 재산, 정보, 서비스를 구매, 임대, 리스, 제공, 교환하도록 유도하거나, 회원에 가입하거나 등록하도록 유도하거나, 상업적 거래를 직·간접적으로 가능하게 하거나, 영향을 미치게 하는 행위와 같이 상업적 또는 경제적 이익을 증진시키는 것을 의미한다. '상업적 목적'에는 정치 연설 및 저널리즘을 포함하여 주 또는 연방 법원이 비상업적 연설로 인정한 연설은 포함되지 않는다(§1798.140 (d)).

(4) 개인정보를 공유한 제3자의 범주

(5) 해당 소비자에 관해서 수집한 특정 개인정보의 항목

소비자는 자신에 관한 정보를 판매하거나[19] '사업(업무) 목적'으로 제공·공개한 사업자에 대해서도 정보의 제공을 요구할 수 있다. 소비자가 개인정보를 판매·제공한 사업자에 대해서 요구할 수 있는 정보는 아래와 같다(1798.115 (a)·(b)).

(1) 소비자에 관해 수집한 개인정보의 범주

(2) 판매한 개인정보의 범주 및 그 개인정보를 구매한 제3자[20]의 범주(제3자의 범주별로 판매한 개인정보의 범주를 각각 구분해서 알려야 한다.)

(3) 사업자가 '사업 목적'으로 제공·공개한 개인정보의 범주

주의해야 할 점은 개인정보 범주의 공개는 개인정보 정의 조항(§1798.140 (a))에서 분류한 개인정보의 유형에 따라 최대한 자세히 설명해야 하고, 개인정보를 제공받거나 공유한 제3자의 범주별로 각각 구분해서 공개해야 한다는 것이다(§1798.130 (a)(3),(4)). 사업자는 동일한 소비자로부터 정보공개 요구를 받은 경우(§1798.110, §1798.115), 12개월 동안 최대 2회까지만 정보를 제공하면 된다(§1798.130 (b)).

19 「캘리포니아주 소비자 프라이버시법(CCPA)」에서 '판매'란 구두, 서면, 전자적 수단, 그밖의 수단을 이용하여 사업자가 다른 사업자 또는 제3자에게 금전적인 가치나 그 밖의 다른 가치를 고려해서 소비자의 개인정보를 판매, 임대, 양도, 제공·공개, 배포, 이전, 조회, 그밖에 제3자가 이용할 수 있게 하는 모든 소통을 의미한다(1798.140 (t)). 금전적(monetary) 가치뿐만 아니라 그밖의 다른 가치(valuable)까지 고려해야 한다는 사실에 유의할 필요가 있다. 소비자의 동의·지시, 인수·합병, 파산 등을 원인으로 한 개인정보 이전은 판매로 보지 아니하며, 사업 목적(business purpose)으로 이용하는 것도 판매로 보지 아니한다.

20 다음 어느 하나에 해당하는 자는 '제3자'로 보지 아니한다(§1798.140 (w)). : (1) 「캘리포니아주 소비자 프라이버시법(CCPA)」에 따라 소비자로부터 개인정보를 수집한 사업자, (2) 서면계약에 따라 사업자가 사업 목적으로 소비자의 개인정보를 공개한 자(수탁자 등). 이 경우 계약서에는 다음의 내용이 포함되어야 한다. i) 개인정보를 제공받는 자가 개인정보를 판매하는 행위, ii) 상업 목적을 위해 개인정보를 보관·이용·공개하는 행위를 포함해 계약서에서 명시한 서비스 이행 이외의 어떤 목적으로 개인정보를 보관·이용·공개하는 행위, iii) 개인정보를 제공받은 자와 사업자 간의 직접적인 업무관계의 범위를 넘어서 정보를 보관·이용·공개하는 행위. 개인정보를 제공받은 자는 i)~iii)의 제한사항을 이해하고 준수할 것이라는 인증을 계약서에 포함해야 한다. 제3자로 보지 아니한 자가 「캘리포니아주 소비자 프라이버시법(CCPA)」에서 명시하고 있는 제한사항을 위반한 경우에는 그 위반자가 위반에 대해서 책임을 진다. 제3자로 보지 아니한 자에게 개인정보를 제공한 사업자는 개인정보를 제공받은 자가 이 법에 명시된 제한사항을 위반하여 개인정보를 이용했더라도 위반에 대한 책임을 지지 아니한다. 다만, 사업자는 개인정보를 제공할 당시 개인정보를 제공받은 자가 그와 같은 위반행위를 저지를 것이라는 사실을 실질적으로 알지 못하거나, 그와 같이 믿을 만한 이유를 가지고 있지 않아야 한다.

3. 개인정보 삭제 요구권

소비자는 사업자에게 자신에 관한 정보의 삭제를 요구할 권리를 가진다(§1798.105 (a)). 사업자는 요구가 정당한 권한을 가진 자에 의한 것임을 확인 가능한 경우에는 소비자의 개인정보를 기록에서 삭제하고, 수탁자에 대해서도 삭제를 지시해야 한다(§1798.105 (c)). 다만, 사업자 또는 수탁자는 해당 개인정보를 보관해야 할 필요가 있는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 소비자의 삭제 요구를 거부할 수 있다(§1798.105(d)).

(1) 계약이행, 서면보증, 연방법에 따른 리콜의무이행, 소비자의 요청이나 소비자와 지속적인 비즈니스 관계 맥락에서 합리적으로 제공이 예상되는 제품 또는 서비스의 제공, 그 밖에 사업자와 소비자 간 계약이행을 위해 필요한 경우

(2) 보안사고의 탐지, 악의적이거나 기만적이거나 사기적이거나 불법적인 활동으로부터의 보호 또는 그와 같은 불법행위에 대해 책임을 져야 할 자의 기소

(3) 기존의 의도된 기능을 손상시키는 오류를 식별하고 복구하기 위해 디버그

(4) 언론의 자유 행사, 언론의 자유권을 행사한 다른 소비자의 권리 보장, 법이 보호하는 다른 권리의 행사

(5) 형법 제2부 제12장 제3.6절에 따른 캘리포니아주 전자통신 프라이버시 보호법의 준수

(6) 소비자가 명시적으로 동의한 경우, 소비자의 삭제 요구로 인해 사업자가 해당 개인정보를 삭제하면 과학적, 역사적 또는 통계적 연구의 목적 달성을 불가능하게 하거나 심각하게 훼손할 가능성이 있는 경우로서 다른 모든 적용 가능한 윤리규범 및 프라이버시 보호 법규를 준수하는 공익 분야에서 공개적(public) 또는 학술적(peer-reviewed) 연구를 수행하는 경우

(7) 소비자와 사업자의 관계를 기반으로 소비자의 기대와 합리적으로 일치하는 범위 내에서 내부적으로만 이용하는 경우

(8) 법적 의무 준수 : 통신 데이터 보관 의무 등

(9) 소비자가 개인정보를 제공한 상황과 양립 가능한 합법적인 방식으로 소비자의 개인정보를 내부적으로 사용하는 경우

사업자는 소비자에게 개인정보의 삭제를 요구할 권리가 있다는 사실을 개인정보보호방침 등에 합리적으로

접근할 수 있는 방식으로 공개해야 한다(§1798.105 (b)). CCPA는 GDPR에 비해 삭제 거부 사유를 매우 광범위하고 구체적으로 규정함으로써 사업자의 입증 부담을 덜어주고 있다.

4. 개인정보 판매 중단 지시권

「캘리포니아주 소비자 프라이버시법(CCPA)」는 사업자가 소비자의 개인정보를 수집·이용하거나 제공·판매할 때 소비자의 사전 동의를 요하고 있지 않다. 대신 소비자는 언제든지 사업자에게 개인정보의 판매 중단을 지시할 권리(이를 'opt-out 권리'라 한다.)를 가진다. 개인정보를 판매하고자 하는 사업자는 소비자에게 미리 해당 개인정보가 판매될 수 있으며, 소비자는 판매를 '거부할 권리'를 가지고 있다는 사실을 합리적으로 접근할 수 있는 방식으로 소비자에게 통지해야 한다(§1798.120 (a)·(b)).

다만, 아동과 청소년에 대해서는 옵트인(opt-in)이 적용된다. 사업자는 소비자가 13세부터 16세 미만인 경우로서 해당 소비자가 16세 미만이라는 사실을 실질적으로 알고 있는 경우에는 해당 소비자의 명확한 승인이 없이 개인정보를 판매할 수 없다. 해당 소비자가 13세 미만인 경우에는 법정대리인 또는 보호자가 확정적으로 승인한 경우가 아니면 개인정보를 판매할 수 없다. 소비자의 나이를 의도적으로 무시한 사업자는 소비자의 나이에 대한 실질적인 지식이 있는 것으로 간주된다(§1798.120 (a)·(c)).

소비자로부터 개인정보 판매 중단 지시를 받은 사업자는 판매 중단 지시를 받은 이후에는 개인정보를 판매해서는 안 되고, 미성년 소비자의 개인정보 판매에 대한 법정대리인 또는 해당 청소년의 동의를 명시적으로 받지 못한 사업자는 처음부터 미성년 소비자의 개인정보 판매가 금지된다(§1798.120 (d)).

다만, 차량 제조자와 판매자가 보유하거나 공유하는 차량 정보(차량번호, 제조자, 모델, 연식, 주행거리 등) 또는 차량 소유자 정보(소유자의 이름, 연락처 등)에 대해서는 그 정보가 법령에 따른 차량 보증 또는 리콜 목적으로 공유되고 다른 목적으로 이용되지 않는 한 판매중단 지시 요구권이 적용되지 않는다(§1798.145 (g)).

「일반개인정보보호규정(GDPR)」 하에서 소비자는 개인정보 판매는 물론 수집, 이용, 제공, 공개 그밖의 모든 처리 활동의 중단 또는 정지를 요구할 수 있음에 비하여 「캘리포니아주 소비자 프라이버시법(CCPA)」는 판매 중단을 지시할 수 있는 권리만을 제한적으로 인정하고 있다.

5. 소비자 권리의 이행 및 거부

사업자는 소비자가 이상과 같은 권리를 요구해 온 경우, 요구를 받은 날부터 45일 이내에 무료로 요구받은 정보를 제공·전달하거나 요구받은 행위를 이행해야 한다. 제공 또는 공개된 정보는 사업자가 요구를 접수받은 날 이전 12개월 동안 처리한 내역을 커버해야 하고, 문서로 제공 또는 공개되어야 한다. 합리적으로 기간연장이 필요한 경우 요구의 복잡성, 요구 건수 등을 고려하여 추가로 45일(총 90일)까지 한 차례 기간을 연장할 수 있다. 이 경우 사업자는 요구 접수 후 45일 이내에 연장 사유를 소비자에게 통지해야 한다(§1798.130 (a)(2), § 1798.145 (i)(1)).

사업자는 소비자의 요구가 정당한 권한을 가진 자[21]에 의한 것인지 여부를 즉시 확인해야 하고 확인이 가능한 경우에 한해서 소비자의 요구를 승인해야 한다. 이를 위해 사업자는 요구받은 개인정보의 성격 등을 고려해서 합리적인 범위 내에서 소비자에게 인증을 요구할 수 있다. 그러나 이를 이유로 소비자에게 계정 설정(회원가입)을 요구해서는 안 된다. 다만, 소비자가 이미 계정을 가지고 있는 경우에는 해당 계정을 통해 권리를 행사하도록 요구할 수 있다(§1798.130 (a)(2)). 정당한 권리자인지 여부를 확인할 목적으로 수집한 개인정보는 확인 목적으로만 이용해야 하고 다른 목적으로 이용할 수 없다(§1798.130 (a)(7)).

사업자가 소비자의 요구를 거부하고자 할 때는 거부 사유, 이의제기권 등을 지체없이 소비자에게 통지해야 한다. 특히, 소비자의 요구가 명백히 근거가 없거나, 과도하거나, 반복적인 경우에 사업자는 정보제공, 통신 등과 같이 요구받은 조치를 취하는데 소요되는 행정비용을 고려해서 합리적인 비용을 부과하거나 거부 사유를 밝히고 요구를 거부할 수 있다. 다만, 명백히 아무 근거가 없고 과도한(manifestly unfounded or excessive) 요구라는 입증책임은 사업자가 부담한다(§1798.145 (i)(2)·(3)).

21 소비자 본인의 신분뿐만 아니라 소비자의 법정대리인 또는 임의대리인의 신분을 포함한다(1798.140 (y)).

Ⅳ. 사업자의 의무

1. 소비자에 대한 정보 고지 의무

소비자의 개인정보를 수집하는 사업자는 개인정보의 수집 시점 또는 그 이전에 소비자에게 수집할 개인정보의 범주와 개인정보의 이용 목적에 대해 알려야 한다. 추가 범주의 개인정보를 수집하거나 수집한 개인정보를 다른 목적으로 이용하려면 소비자에게 추가 수집할 개인정보의 범주 및 개인정보의 추가 이용 목적을 다시 알려야 하며, 추가 정보를 제공하지 않고는 추가 범주의 개인정보를 수집하거나 수집한 개인정보를 다른 목적으로 이용할 수 없다(§1798.100 (b)).

또한, 제3자가 수집 시의 약속과 실질적으로 일치하지 않는 방식으로 소비자의 개인정보를 이용하거나 공유하는 방법을 중대하게 변경하려면, 소비자에게 새로운 또는 변경된 방식을 미리 통지해야 한다. 이 경우 통지는 소비자가 쉽게 판매 중단을 선택할 수 있도록 충분히 눈에 띄고 확실하게 행해져야 한다(§1798.140 (t)(2)(D)).

「일반개인정보보호규정(GDPR)」과 달리 수집할 개인정보의 구체적 항목은 고지 의무의 대상이 아니며, 개인정보의 보관기간, 개인정보보호책임자의 연락처, 감독당국에 대한 민원제기권 등도 고지 대상이 아니다.

2. 손쉬운 권리행사 수단 제공 의무

사업자는 소비자가 정보열람 요구, 정보공개 요구 등 자신의 권리를 행사할 수 있도록 신뢰할 수 있는 확인 수단을 제공하여야 한다. 그러나 소비자 인증을 이유로 소비자에게 계정의 신설을 요구해서는 안 된다(§1798.130 (a)(2)).

사업자는 소비자가 쉽게 정보제공 요구권을 할 수 있도록 합리적으로 접근할 수 있는 방식으로 최소한 무료 전화번호를 포함한 두 개 이상의 방법을 제공해야 한다.[22] 다만, 사업자가 온라인으로만 사업을 운영하고 있고

22 이와 같은 권리 행사 방법으로는 우편주소, 전자우편주소, 인터넷 웹페이지, 인터넷 웹포털, 무료 전화번호, 그 밖에 소비자가 사업자에게 쉽게 연락을 취할 수 있는 편리한 접근수단으로써 주 법무장관이 승인한 연락처 등이 있다(§1798.140 (i)).

소비자와 직접적인 관계를 가지고 있는 경우라면 정보공개 요구권을 행사할 수 있는 방법으로 이메일주소 하나만 제공해도 된다. 또한 사업자가 인터넷 웹사이트를 운영하고 있는 경우에는 소비자가 인터넷 웹사이트를 통해서 정보공개 요구를 신청할 수 있는 조치를 마련해야 한다(§1798.130 (a)(1)).

3. 개인정보처리방침 등 작성·공개 의무

사업자가 온라인 개인정보보호방침을 가지고 있다면 소비자가 합리적으로 접근할 수 있는 형태로 온라인 개인정보보호방침에 아래의 모든 정보를 공개해야 하고, 캘리포니아주 소비자 개인정보권리 설명서에도 소비자가 합리적으로 접근할 수 있는 형태로 아래의 모든 정보를 공개해야 한다. 사업자가 개인정보보호방침을 가지고 있지 않다면, 인터넷 웹사이트에 소비자가 합리적으로 접근할 수 있는 형태로 다음의 정보를 공개해야 한다(§1798.130 (a)(5), §1798.110 (c), §1798.115 (c)).

(1) 소비자의 권리(개인정보 열람·사본 제공 요구권, 개인정보 삭제 요구권, 개인정보 수집·판매에 대한 정보 제공 요구권, 차별 취급을 받지 않을 권리)에 대한 설명

(2) 소비자가 권리를 요구할 수 있는 하나 이상의 지정된 방법

(3) 개인정보 수집·이용에 관한 정보(§1798.110 (c))
- 수집한 개인정보의 범주
- 개인정보의 수집 출처 : 온라인 주문기록, 온라인 서베이, 마케팅 회사, 쿠키, 웹비콘, 트레킹 픽셀, 모집인 등
- 개인정보를 수집하거나 판매한 사업 목적 또는 상업 목적 : 사기방지, 마케팅, 소비자 경험 개선 등
- 개인정보를 공유한 제3자의 범주 : 맞춤형 광고 파트너, 계열사, 소셜미디어 웹사이트, 수탁자 등
- 수집한 개인정보의 구체적 항목

(4) 개인정보 판매·제공에 관한 정보(§1798.115 (c))
- 판매한 개인정보의 범주(판매하지 아니한 경우에는 판매하지 않은 사실)
- 사업 목적으로 제공·공개한 개인정보의 범주(사업 목적으로 제공·공개하지 아니한 경우에는 사실)

이 경우 공개 대상 개인정보는 사업자가 이전 12개월 동안 수집·판매·제공한 것에 한하며, 최소한 12 개월마다 한 번씩 해당 정보를 업데이트해야 한다(§1798.130 (a)(5)(B)·(C)). 또한, 개인정보의 범주는 수집·판매·

제공한 개인정보를 최대한 자세히 설명할 수 있도록 개인정보 정의 조항(§1798.140)에서 분류하고 있는 개인정보의 유형에 따라 공개해야 한다.

「캘리포니아주 소비자 프라이버시법(CCPA)」는 「일반개인정보보호규정(GDPR)」과 달리 쿠키를 통해 수집하는 개인정보의 수집·이용과 관련하여 별도의 쿠키 정책을 작성·공개하도록 요구하고 있지는 않으며, 소비자에게 쿠키를 통한 개인정보 수집 활동에 대하여 별도의 권리를 인정하고 있지도 않다. 따라서 쿠키 정책은 개인정보보호방침에 포함하면 된다.[23)]

4. 기술적·관리적 보호조치 의무

「캘리포니아주 소비자 프라이버시법(CCPA)」는 일반개인정보보호규정(GDPR)과 달리 사업자에게 명시적으로 개인정보보호를 위한 기술적·관리적 조치의무를 부여하고 있는 규정을 두고 있지 않다. 다만, 사업자가 정보의 성격에 따라 개인정보를 적절하고 합리적인 보안 절차와 관행을 이행하고 유지해야 할 의무를 위반한 결과 암호화, 부분삭제 등 비식별 조치가 되지 아니한 개인정보가 유출·도난·공개되거나 무단으로 접근된 경우에는 실제손해배상책임은 물론 법정손해배상책임도 져야 할 수 있다 (§1798.150 (a)).

「캘리포니아주 소비자 프라이버시법(CCPA)」 하에서 개인정보의 성격에 따라 암호화, 부분삭제 등 '합리적으로' 요구되는 보호조치란 (i) 사회보장번호, (ii) 운전면허 번호 또는 캘리포니아주 주민카드 번호, (iii) 계정번호·신용카드번호·직불카드번호(개인의 금융계정에 접근하기 위해 필요한 보안코드, 접속코드, 비밀번호 등이 결합되어 있는 경우), (iv) 의료정보, (v) 소비자의 이름을 암호화(encrypted)하거나 부분 삭제한(redacted) 것을 의미한다(§1798.81.5 (d)(1)(A)).

23 California Consumer Privacy Act FAQs for Covered Businesses.

5. 소비자에 대한 차별 금지 의무

사업자는 소비자가 「캘리포니아주 소비자 프라이버시법(CCPA)」에 따른 소비자의 권리를 행사했다는 이유로 해당 소비자에 대해서 (1) 상품 또는 서비스의 제공을 거부하거나, (2) 할인 또는 그 밖의 혜택의 제공, 위약금(penalties) 부과 등을 포함해 다른 가격 또는 요율을 적용하거나, (3) 수준이나 품질이 다른 상품 또는 서비스를 제공하는 등 어떤 차별행위도 해서도 안 된다. 또한, 소비자에게 다른 가격 또는 요율이 적용되거나 다른 수준 또는 품질의 상품이나 서비스가 제공될 수 있음을 암시해서도 안 된다(§1798.125 (a)(1)). 다만, 사업자가 소비자에게 다른 가격 또는 요율을 적용되거나 다른 수준 또는 품질의 상품이나 서비스를 제공하더라도 그 같은 차이 또는 차별이 사업자가 소비자의 데이터로부터 얻게 되는 가치와 '합리적으로' 관련되어 있다면 예외적으로 차별 적용이 허용된다(§1798.125 (a)(2)).

또한 사업자는 개인정보 수집·판매·삭제에 대한 보상으로 소비자에게 대가의 지불을 포함해 금전적 인센티브를 제공할 수 있고, 소비자에게 제공되는 상품 또는 서비스의 가격이나 품질의 차이가 사업자가 소비자의 데이터로부터 얻게 되는 가치와 '직접적으로' 관련되어 있다면, 다른 가격·요율·수준품질을 적용할 수 있다(§1798.125 (b)(1)). 사업자가 금전적 인센티브를 제공하는 경우에는 개인정보보호방침 등을 통해서 합리적으로 접근할 수 있는 형태로 소비자에게 금전적 인센티브를 알려야 하고, 금전적 인센티브 프로그램의 중요한 조건과 언제든지 행사 가능한 소비자의 취소권을 명확히 알리고 소비자의 사전 동의를 얻은 경우에만 인센티브 프로그램에 해당 소비자를 참여시킬 수 있다(§1798.125 (b)(2)(3)).

그러나 어느 경우에도 사업자는 소비자가 「캘리포니아주 소비자 프라이버시법(CCPA)」에 따른 소비자의 권리를 행사했다는 이유로 해당 소비자에 대해서 상품 또는 서비스의 제공을 거부하지는 못하며(§1798.125 (a)(1)), 성격상 부당하거나, 불합리하거나, 강제적거나, 착취적인(usuious) 인센티브 관행을 이용해서는 안 된다(§1798.125 (b)(4)).

「일반개인정보보호규정(GDPR)」에서도 '개인정보의 공정처리원칙(§5.1 (a))'에 따라 정보주체에게 권리 행사를 이유로 불합리한 차별을 하는 것은 금지되는 것으로 해석되고 있으나, 「캘리포니아주 소비자 프라이버시법(CCPA)」는 이를 구체적으로 명시하고 있다는 점에서 차이가 있다.

6. 개인정보 판매 금지·중단 의무

사업자는 소비자로부터 개인정보 판매 중단 지시를 받은 경우에는 판매를 중단해야 하며, 소비자가 합리적으로 이용할 수 있는 방식으로 아래의 의무를 준수해야 한다(§1798.135 (a)).

(1) 판매 중단 링크 제공 의무 : 소비자 또는 소비자가 위임한 자가 이용할 수 있는 인터넷 홈페이지 위에 ‘“내 개인정보 판매 금지하기(Do Not Sell My Personal Information)”’라는 제목으로 명확하고 눈에 잘 띄는 링크를 제공할 것

(2) 설명 제공 의무 : 온라인 개인정보보호 방침(가지고 있는 경우)과 캘리포니아주 소비자 개인정보권리 설명서에 소비자의 개인정보 판매 중단 지시권을 설명할 것(링크를 통해 ‘“내 개인정보 판매 금지하기”’ 인터넷 웹페이지로 연결)

(3) 계정 신설 요구 금지 의무 : 개인정보 판매 중단 지시권을 접수받을 목적으로 계정 신설(회원 가입)을 요구하지 않을 것

(4) 개인정보취급자 등에 대한 숙지 의무 : 「캘리포니아주 소비자 프라이버시법(CCPA)」의 준수에 대해서 책임을 지고 있거나 개인정보와 관련한 소비자의 민원(문의)을 다루고 있는 모든 임직원에게 소비자의 개인정보 판매 중단 지시권, 판매 중단 지시와 관련한 사업자의 의무, 소비자가 판매 중단 지시권을 행사하기 위한 방법 등을 충분히 인지하도록 보장할 것

(5) 개인정보 판매승인 요청 제한 : 판매 중단 지시를 받은 날부터 12개월 내에는 다시 판매 승인을 요청하지 않을 것

(6) 개인정보의 목적 외 이용 금지 : 판매 중단 지시를 받을 때 수집한 개인정보는 지시 의무 준수 목적으로만 이용하고 다른 목적으로 이용하지 않을 것

사업자가 캘리포니아주 소비자를 대상으로 개인정보 판매 중단 지시 링크와 판매 중단 지시권에 관한 설명이 포함된 별도의 추가적인 홈페이지를 운영하고 있다면 그리고 캘리포니아주 소비자가 해당 홈페이지에 접속하도록 합리적인 조치를 취하고 있다면, 사업자는 일반 대중이 이용할 수 있도록 운영하고 있는 홈페이지에 판매 중단 지시 링크와 설명을 포함할 필요는 없다(§1798.135 (b)).

소비자는 다른 사람에게 판매 중단 지시권(opt-out)의 행사를 위탁할 수 있고, 사업자는 수탁자로부

터 주 법무장관이 제정한 시행규칙으로 정한 방법에 따라 판매 중단 지시를 받으면 그 지시에 따라야 한다(§1798.135 (c)).

소비자가 명시적으로 판매 중단 지시권에 대한 고지·설명을 듣고 중단 지시권을 행사할 수 있는 기회를 제공받지 않는 한, 사업자로부터 개인정보를 제공받은 제3자는 사업자가 자신에게 판매한 소비자의 개인정보를 재판매해서는 안 된다(§1798.115 (d)).

7. 위·수탁 계약의 체결 의무

사업자(위탁자)로부터 개인정보를 제공받은 수탁자가 「캘리포니아주 소비자 프라이버시법(CCPA)」의 의무를 위반했더라도 해당 개인정보를 제공할 당시 수탁자가 그와 같은 위반행위를 하려는 의도가 있다는 사실을 실질적으로 몰랐거나 그와 같이 믿는데 이유가 있다면, 사업자는 수탁자의 법 위반에 대해서 책임을 지지 않는다(§1798.145 (j)).

사업자가 수탁자에게 개인정보 처리업무를 위탁하고자 하는 경우, 사업자는 수탁자와 문서로 된 계약을 체결해야 하고, 해당 계약서에는 위탁업무처리 목적 외 개인정보의 보관·이용·제공·공개 등을 금지하는 내용이 포함되어야 한다(§1798.140 (v)).

8. 개인정보취급자 등에 대한 숙지 의무

사업자는 「캘리포니아주 소비자 프라이버시법(CCPA)」의 준수에 대해서 책임을 지고 있거나 개인정보와 관련한 소비자의 민원(문의)을 다루고 있는 모든 임직원이 소비자의 권리와 의무에 관한 사항, 소비자가 자신의 권리를 행사할 수 있는 방법, 사업자의 책임과 의무 등을 충분히 이해할 수 있도록 소비자의 개인정보 열람권 및 이동권(§1798.100), 개인정보 삭제요구권(§1798.105), 수집 개인정보의 처리에 관한 정보공개 요구권(§1798.110), 판매 개인정보의 처리에 관한 정보공개 요구권(§1798.115), 개인정보 판매 중단 지시권(§1798.125), 소비자의 권리의 행사 및 이행 방법과 절차(§1798.130) 등을 숙지시켜야 한다(§1798.130 (a)(6)).

V. 법위반에 대한 제재 및 피해구제

1. 손해배상청구 등 소비자의 민사소송

사업자가 개인정보를 보호하기 위해 정보의 성격에 따라 적절하고 합리적인 보호조치를 해야 할 의무[24]를 위반함으로써 개인정보가 암호화, 부분삭제(redacting) 등이 되지 아니한 상태로 권한이 없는 자에 의하여 무단 접근되거나 유출·도난·공개된 경우 소비자는 개인적으로 또는 집단적으로 손해배상(법정손해배상 또는 실제손해배상), 금지명령(injunctive relief), 확인의 소(declaratory relief), 기타 법원이 적절하다고 판단한 소를 제기할 수 있다(§1798.150 (a)(1)).

소비자는 실제손해배상액과 사건(incident) 당 소비자 당 100~750 달러의 법정손해배상액 중 높은 금액을 손해배상액으로 청구할 수 있다. 다만, 소비자가 법정손해배상을 구하는 개인소송 또는 집단소송을 제기하려면 30일 전에 사업자가 위반했다고 생각하는 「캘리포니아주 소비자 프라이버시법(CCPA)」의 해당 조항을 서면으로 통지하여야 한다(이른바 thirty days' notice). 사업자가 30일 이내에 통지받은 법위반 사항을 치유하고 더 이상 위반행위가 재발하지 않을 것이라는 사실을 입증하는 명시적인 서면 회신(express written statement)을 제출한 경우 소비자는 법정손해배상청구 소송을 제기할 수 없다(§1798.150 (b)).

사업자가 30일 이내에 소비자에게 통지받은 법위반 사항을 치유하고 더 이상 위반행위가 재발하지 않을 것이라는 사실을 입증하는 명시적인 서면 회신을 제출하지 아니하고 계속해서 법을 위반한 경우, 소비자는 사업자에게 서면회신을 강제하기 위반 소를 제기할 수 있고 명시적인 서면회신 의무를 위반할 때마다 법정손해배상 청구 소송을 제기할 수 있다(§1798.150 (b)).

법정손해배상의 경우 소비자는 자신이 입은 피해를 입증할 필요가 없지만, 법원이 법정손해배상액을 평가할 때는 위법행위의 성격과 심각성, 위반 횟수, 위법행위의 지속성, 위법행위가 발생한 기간, 위법행위의 고의성,

24 개인정보의 성격에 따라 '합리적으로' 요구되는 보호조치란 (i) 사회보장번호, (ii) 운전면허 번호 또는 캘리포니아주 주민카드 번호, (iii) 계정번호·신용카드번호·직불카드번호(개인의 금융계정에 접근하기 위해 필요한 보안코드, 접속코드, 비밀번호 등이 결합되어 있는 경우), (iv) 의료정보, (v) 소비자의 이름(first name or first initial and last name)을 암호화(encrypted)하거나 부분삭제한(redacted) 것을 의미한다(§1798.81.5 (d)(1)(A)).

피고의 자산·부채·순자산 등을 포함하여(이에 한정되지 아니한다.), 소송 당사자가 제시한 관련 상황 중 하나 이상을 고려해야 한다(§1798.150 (a)(2)).

30일 이내에 위반 사항을 치유한 경우, 사업자는 법정손해배상책임을 면하게 되지만, 소비자에게 실제 피해가 발생한 경우에는 실제손해에 대한 배상책임은 피할 수 없다. 또한, 개별 소비자가 「캘리포니아주 소비자 프라이버시법(CCPA)」 위반을 이유로 실제 발생한 금전적 피해에 대해서만 소송을 제기한 경우에는 30일 전 사전 통지가 요구되지 아니한다(§1798.150 (b)).

「캘리포니아주 소비자 프라이버시법(CCPA)」 §1798.150에 따른 민사소송(법정손해배상, 단체소송, 금지명령, 확인의 소)은 사업자의 보호조치의무 위반에 따른 개인정보의 무단접근·유출·도난·공개에 대해서만 적용되고, 이 법 「캘리포니아주 소비자 프라이버시법(CCPA)」의 다른 조항 위반에 대해서는 적용되지 않는다(§1798.150 (c)).

2. 주 법무장관의 민사벌금 부과

주 법무장관은 사업자에게 법 위반을 통지할 수 있다. 사업자가 「캘리포니아주 소비자 프라이버시법(CCPA)」 미준수를 통지받은 후 30일 이내에 위반행위를 시정하지 않으면, 최종적으로 이 법을 「캘리포니아주 소비자 프라이버시법(CCPA)」 위반한 것이 된다. 「캘리포니아주 소비자 프라이버시법(CCPA)」를 위반한 사업자, 수탁자, 그 밖의 위반자는 금지명령에 따라야 하고, 각각의 위반에 대하여 2,500 달러 이하의 민사벌금(civil penalty)을 부과받게 된다. 예컨대, 10명의 소비자 정보를 불법 판매한 경우, 최고 2만5천 달러의 과징금이 부과된다(on a per-capita basis). 그러나 1명의 소비자 정보를 여러 차례 반복해서 판매한 경우에는 전체를 1건으로 처리한다. 고의적인 위반에 대해서는 각각의 위반에 대하여 3배인 7,500 달러의 민사벌금에 처해진다. 민사벌금은 주 법무장관이 캘리포니아주 주민들의 이름으로 제기한 민사소송에서 배타적으로 다루어지게 된다(§1798.155 (b)).

사업자는 주 검찰총장으로부터 법 위반을 통지를 받은 날부터 30일 이내에 위반 사항을 치유할 수 있다. 사업자가 법 위반 통지를 받고 30일 이내에 위반행위를 치유하지 않은 경우에 한해 민사벌금이 부과된다. 민사벌금은 위반행위의 성격, 지속 여부, 위반 기간, 고의성, 심각성 등을 고려해서 결정된다.

「캘리포니아주 소비자 프라이버시법(CCPA)」 위반에 대해서 평가된 민사벌금과 소송 합의금은 이 법 「캘리포니아주 소비자 프라이버시법(CCPA)」 집행과 관련해서 주 법원 및 법무장관에 의해 발생한 모든 비용을 충당하기 위하여 캘리포니아주 일반기금 내에 새로 설치된 '소비자 프라이버시 기금'에 예치된다(§1798.155 (c)).

Ⅵ. 「캘리포니아주 소비자 프라이버시법(CCPA)」의 영향 및 시사점

1. 국내 기업에 대한 「캘리포니아주 소비자 프라이버시법(CCPA)」의 영향

캘리포니아주는 미국에서 인구가 가장 많은 주 중 하나이자 국내 기업들이 많이 진출해 있는 곳이기도 한다. 캘리포니아주에서 직접 사업을 하고 있지 않은 국내 기업이라도 캘리포니아주 소비자(주민, 근로자, 거래처 등)의 개인정보를 수집·이용·제공하면 「캘리포니아주 소비자 프라이버시법(CCPA)」의 적용을 받게 된다. 예컨대, 국내 게임회사나 전자상거래업체가 캘리포니아주 주민과 전자상거래를 하거나, 국내 가전제품 제조회사나 자동차 제조사가 TV, 세탁기, 냉장고, 스마트워치, 스피커, 자동차 등의 IoT 기기를 이용하여 국내에서 캘리포니아주 주민의 개인정보를 수집·이용하려면, 「캘리포니아주 소비자 프라이버시법(CCPA)」를 준수해야 한다.

「캘리포니아주 소비자 프라이버시법(CCPA)」의 각종 규제는 국내법 및 「일반개인정보보호규정(GDPR)」과 상당한 차이가 있다. 따라서 국내법과 GDPR을 충실히 준수해온 기업이라도 「캘리포니아주 소비자 프라이버시법(CCPA)」를 위반할 수 있다. 먼저, 「캘리포니아주 소비자 프라이버시법(CCPA)」에서의 개인정보의 정의와 범위는 국내에서 이해되고 있는 것보다 훨씬 넓게 규정되어 있고, 어떤 면에서 보면 유럽연합 GDPR보다 더 넓다고 할 수도 있다. 또한, 국내법에 따라 개인정보처리에 대해서 사전 동의를 받고 있는 국내 기업이라도 「캘리포니아주 소비자 프라이버시법(CCPA)」에 따라 '내 정보 판매 중단하기(Do Not Sell My Personal Information)' 링크를 제공해야 하고, 소비자의 정보이동권 행사에 대해서도 대비를 해야 한다.

국내에서는 개인정보처리에 대한 동의를 거부한 정보주체에 대해서 상품 및 서비스 제공 거부만 금지되지만, 「캘리포니아주 소비자 프라이버시법(CCPA)」에서는 가격, 품질 등의 차별을 포함하여 모든 유형의 차별이

금지된다. 개인정보보호방침 등에 공개해야 할 정보의 내용에도 차이가 있고 공개 방법에도 차이가 있다. 특히, 무료 전화번호를 포함하여 소비자가 자신의 권리를 쉽게 행사할 수 있는 조치를 강구해야 한다. GDPR과 같이 글로벌 매출액을 기준으로 하는 천문학적인 과징금제도는 없지만, 고액의 법정손해배상제도를 포함하여 집단소송, 금지명령, 확인의 소 등 다양한 민사소송제도를 마련해 두고 있다. 게다가 고액의 민사벌금제도가 마련되어 있다. 사업자에게 thirty days' notice의 기회가 주어지기는 하지만, 사업자는 항상 집단소송 등의 위험에 대비하지 않으면 안 된다.

2. 국내 개인정보보호제도에 대한 시사점

미국의 「캘리포니아주 소비자 프라이버시법(CCPA)」는 국내법과 법체계가 다르지만, AI와 IoT 등으로 대변되는 데이터 경제시대에 우리나라가 벤치마킹할 수 있는 독창적인 제도를 많이 마련해 두고 있다. 「캘리포니아주 소비자 프라이버시법(CCPA)」의 가장 큰 특징은 개인정보의 활용 목적을 '사업(업무) 목적'과 '상업 목적'으로 나누고, 개인정보의 처리도 수집·이용과 판매·제공을 구분하여 각각 규제와 보호 수준을 달리 규정하고 있다는 점이다.

「캘리포니아주 소비자 프라이버시법(CCPA)」에서 '사업(업무) 목적'의 개인정보 이용·제공이란 국내법상 개인정보처리자의 '정당한 이익' 추구를 위한 개인정보처리와 유사한 개념이라고 할 수 있다. 국내에서는 '정당한 이익' 추구가 매우 좁게 해석되고 있는 반면, 「캘리포니아주 소비자 프라이버시법(CCPA)」는 '사업 목적'을 매우 광범위하게 규정하고 있다. 보안사고 탐지, 서비스의 이행, 오류의 식별·복구를 위한 디버깅 외에 기술 개발 및 실증을 위한 내부적 연구, 품질 또는 안전성의 확인·관리를 위한 활동, 서비스의 개선·업그레이드 및 향상, 소비자와 실시간 상호작용 및 동시 거래에 대한 모니터링 등도 '사업 목적'에 포함시킴으로써 개인정보처리와 관련해서 사업자와 소비자의 이익을 조화시키고 있다.

또한 「캘리포니아주 소비자 프라이버시법(CCPA)」는 GDPR과 마찬가지로 개인정보 열람권, 정보이동권 등을 보장하고 있고 소비자가 쉽게 자신의 권리를 행사할 수 있는 조치를 마련하도록 하는 의무를 부과하고 있다. 하지만 최근 12개월 내에 처리한 개인정보로 권리행사의 범위를 제한하고 있으며 소비자가 권리를 행사할 수 있는 횟수도 1년에 2회 이내로 제한하고 있다. 또한 정보이동권의 경우에도 소비자 자신 이외에 다른 사업자에 대한 이동 지시권은 허용하지 않음으로써 사업자의 부담을 경감시키고 있다.

「캘리포니아주 소비자 프라이버시법(CCPA)」는 실질손해배상, 법정손해배상, 집단소송, 금지명령, 확인의 소 등 다양한 권리침해 구제제도와 고액의 민사벌금제도를 도입하고 있다. 하지만 법정손해배상은 암호화, 부분삭제 등의 비식별 조치가 되어 있지 않은 개인정보가 유출, 분실, 도난, 무단 접근된 경우로 제한하고 있고, thirty days' notice제도를 도입함으로써 사업자가 과도한 소송 위험이나 민사벌금에 노출되지 않도록 배려하고 있다.

한편, 「캘리포니아주 소비자 프라이버시법(CCPA)」는 소비자의 권리행사를 이유로 한 차별대우를 금지하고, 소비자의 권리포기 규정 등 소비자에게 불리한 계약의 효력을 무효로 규정하는 한편, 개인정보처리와 관련하여 「캘리포니아주 소비자 프라이버시법(CCPA)」와 다른 법률의 규정이 충돌하는 경우에는 소비자에게 가장 유리한 법률을 적용하도록 법의 적용순서를 명시함으로써 소비자의 권리보호에도 세심하게 배려하고 있다. 또한 소비자로부터 개인정보 판매 중단 요구를 받은 경우, 사업자는 해당 개인정보를 구입하거나 제공받은 자에게 소비자의 판매 중단 요구를 알리도록 하는 등 소비자보호제도의 실효성 확보에도 세심한 배려를 하고 있다.

「캘리포니아주 소비자 프라이버시법(CCPA)」는 현재 시행규칙이 입법 예고되어 의견수렴에 들어간 상태이다. 시행규칙에서는 법률에서 담지 못한 보다 디테일한 사항이 많이 포함될 것으로 예상된다.

참고문헌

- Testimony of Alastair Mactaggart, United States Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, Wednesday, October 10th, 2018 (https://www.commerce.senate.gov/services/files/9CC53419-6E09-4075-98BA-4C4F2D46A686).
- California Consumer Privacy Act (CCPA): What you need to know to be compliant(https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html).
- What is a 'consumer' under the CCPA? Dec 1, 2018 (https://medium.com/golden-data/what-is-a-consumer-under-the-ccpa-fcdcfec776f0).
- Are You Prepared for the California Consumer Privacy Act? Get Ready for European-Style Privacy in the U.S. (https://www.pepperlaw.com/events/are-you-prepared-for-the-california-consumer-privacy-act-get-ready-for-european-style-privacy-in-the-us-2018-09-07/).
- California Consumer Privacy Act FAQs for Covered Businesses (https://www.jacksonlewis.com/publication/california-consumer-privacy-act-faqs-covered-businesses).
- California Governor signs all 5 CCPA amendments (https://www.dataprotectionreport.com/2019/10/california-governor-signs-all-5-ccpa-amendments/).
- Mic Drop : California AG releases long-awaited CCPA Rulemaking (https://www.dataprotectionreport.com/2019/10/mic-drop-california-ag-releases-long-awaited-ccpa-rulemaking/).
- The billionaire behind California's sweeping new data privacy law reveals his plans to further regulate the ad industry and fight big tech lobbyists(https://www.businessinsider.in/advertising/news/the-billionaire-behind-californias-sweeping-new-data-privacy-law-reveals-his-plans-to-further-regulate-the-ad-industry-and-fight-big-tech-lobbyists/articleshow/72009163.cms).