

해외 개인정보보호 동향 보고서

최신동향 보고서 2019년 2월 2주

해외의 아동 개인정보 수집 및 이용에 관한 동의 관행 및 법제 동향

< 목 차 >

1. 개요

2. 주요 해외 법제 사례

- (1) 미국의 「아동 온라인 개인정보 보호법(COPPA)」
- (2) EU의 「GDPR」 및 관련 가이드라인
- (3) 프랑스의 「데이터 보호법」
- (4) EU집행위원회의 「모바일 헬스케어 앱 개발자 대상 개인정보보호 행동지침」

3. 시사점

1. 개요

- ▶ 아동 개인정보보호의 중요성과 특수성을 고려하여 온라인에서 아동의 개인정보 수집 및 이용에 대한 기준이 필요
 - 개인정보의 처리를 위해서는 법령에 의해 허용되거나 충분한 정보와 이에 대한 이해에 입각한 정보주체의 동의(informed consent)가 필요하다는 개인정보보호의 기본원칙이 아동의 경우에도 동일하게 적용
 - 그러나 자기결정 능력이 미숙한 아동이 숙려되지 않은 상태에서 개인정보 이용에 대해 동의함으로써 개인정보 침해로 인한 다양한 위험을 초래하거나 재산상의 불이익을 유발할 가능성에 주목
 - 특히 정보기술 환경의 급격한 변화에 따라 각종 사물인터넷(IoT) 기기와 스마트스피커 등을 통한 아동의 개인정보보호 노출 가능성이 더욱 커지고 있는 상황
 - 이에 따라 온라인 및 새로운 정보기술 공간에서 아동을 보호하려는 노력의 일환으로 법정대리인의 동의 없는 아동의 개인정보 수집 및 이용을 제한하고, 새로운 기술 환경에서 아동의 개인정보 동의와 관련된 사항을 규율하는 것이 중요
 - 단, 주요국에서 아동 개인정보보호에 관한 특별법적 규정이 있는 경우는 미국의 COPPA가

2019년 2월 2주

거의 유일하며, 일반 개인정보보호법제가 아동의 경우에도 적용되고 있는 상황

2. 주요 법제 사례

(1) 미국의 「아동 온라인 개인정보 보호법(Children's Online Privacy Protection Act, 'COPPA)」¹

- ▶ 미 연방법으로 제정된 「아동 온라인 개인정보 보호법(Children's Online Privacy Protection Act, 'COPPA)」은 온라인상에서 수집·이용·공개되는 13세 미만 아동의 개인정보에 대해 부모에게 통제 권한을 부여함으로써, 해당 정보에 대한 불공정 행위 또는 관행을 제재
 - 아동의 개인정보를 수집·이용·공개하기에 앞서 ▲증명 가능한 부모의 동의(verifiable parental consent)²를 받아야 하며 ▲동의 이후 개인정보 처리 관행에 주요한 변경이 있는 경우에는³ 다시 동의를 받도록 규정
 - 제3자가 아동의 개인정보를 수집하는 경우에 대해서도 웹사이트와 온라인서비스가 부모에게 고지하고 동의를 받을 의무가 있다고 규정⁴
 - 한편, COPPA는 아동의 개인정보 수집·이용·공개 등과 관련하여 불공정하거나 기망하는 행위를 방지하기 위해 미 연방거래위원회(FTC)에게 아동의 온라인 프라이버시 보호를 위한 규칙 공표 및 집행 권한을 부여
- ▶ FTC는 COPPA의 구체적인 사항을 명시한 「COPPA 규칙(Children's Online Privacy Protection Act)」⁵을 통해 13세 미만 아동의 개인정보에 대한 수집·이용·공개 시 웹사이트/온라인 서비스 운영자가 온라인 프라이버시 보호를 위해 준수해야 할 사항을 제시
 - 웹 사이트나 앱에서 13세 이하 어린이의 개인 정보를 수집하기 전에 부모의 동의를 얻도록 하는 이 규칙은 2013년 웹사이트나 온라인 서비스에서 수집하는 13세 이하 어린이의 개인정보에 대한 부모의 통제권을 강화하도록 개정
 - COPPA 규칙은 ▲13세 미만 아동의 개인정보를 수집·이용·공개하는 웹사이트 또는 온라인 서비스 제공자에 대해 적용되며 ▲온라인 서비스가 일반인을 대상으로 하더라도 13세

1 <http://www.coppa.org/coppa.htm>

<https://www.law.cornell.edu/uscode/text/15/chapter-91>

2 개인정보 관련 통지에 설명된 미래의 개인정보 수집, 이용, 공개에 대한 승인 요청을 위해 가능한 기술을 포함한 합당한 노력(any reasonable effort)을 기울여야 함을 의미 (출처: <http://www.coppa.org/coppa.htm>)

3 부모가 동의한 사항이 변경되면 업데이트된 고지내용(Notice)을 직접 송부해야 함

4 <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>

5 <https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5>

미만의 아동 개인정보를 수집하고 있다는 점을 알고 있는 경우도 해당⁶

- 이 규칙은 ▲ 웹 사이트 또는 온라인 서비스에 대한 고지(§312.4 (d)) ▲부모나 보호자의 사전 동의 획득(§312.5)⁷ ▲아동이 온라인 사업자에 제공한 개인정보를 검토할 수 있는 부모의 열람·제공·삭제 요청권(§312.6) 등을 보장

▶ FTC는 「사업자를 위한 COPPA 규칙 가이드(COPPA Rule : A Six-Step Compliance Plan for Your Business)⁸」를 통해 급변하는 개인정보보호 환경을 반영하여 부모의 동의를 획득하는 새로운 방법을 추가

- 아동의 개인정보 수집을 위한 부모의 동의 확보 방법과 관련하여 ▲지식기반의 질의 인증(Knowledge-based Challenge Questions) 및 ▲안면인식 기술을 활용한 ‘사진 ID(Photo ID)’ 대조 방식을 새롭게 추가
 - 동의 획득 방법은 사업자에 일임하되 동의하는 사람이 아동의 부모라는 점을 증명할 수 있도록 부모의 동의는 다음과 같은 방식으로 진행
 - a. 부모가 동의서에 서명한 후 팩스, 우편, 전자 스캔으로 송부
 - b. 온라인 결제를 하는 사업자의 경우, 거래 내역 통지가 가능한 신용카드나 기타 온라인 지불 시스템을 활용하여 동의(결제)하는 사람이 해당 아동의 부모인지를 증명
 - c. 정부에서 발행한 신분증 사본을 제공
 - d. 부모가 아닌 경우 응답하기 어려운 ‘지식기반 질의(Knowledge-based Challenge Questions)’에 대한 답변을 통해 부모 본인을 인증
 - e. 얼굴인식 기술을 활용해 부모가 사전 등록한 신분증 사진과 추후 제출하는 사진을 비교하여 부모를 인증
- 이 가이드는 COPPA 준수와 관련하여 증명 가능한 부모 동의를 획득하는 것이 어려웠던 문제를 해결하기 위해 부담을 경감하는 방안 강구함으로써⁹ 기업이 좀 더 용이하게 부모 동의 방법을 적용할 수 있도록 융통성 부여한 것으로 평가¹⁰

▶ 한편, COPPA 규칙에 대한 세이프 하버 프로그램의¹¹ 2017년 수정 버전¹²에서는 웹사이트

6 단, 「사업자를 위한 COPPA 규칙 가이드(COPPA Rule : A Six-Step Compliance Plan for Your Business)에 따르면, 웹사이트가 아동을 주된 이용자로 설정하지 않더라도 위 요소에 따라 13세 미만 아동을 대상으로 할 경우에는 13세 미만 이용자에 대해서만 COPPA를 적용할지 것인지 여부를 선택할 수 있음

7 An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

8 <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>

9 <http://www.lexology.com/library/detail.aspx?g=1dce7f61-f82b-4f45-a9f3-83a920d464ee>

10 <https://www.lexology.com/library/detail.aspx?g=5c1b6835-dec5-4c6c-8200-1baaad3cd236>

11 FTC의 COPPA 규칙에는 산업단체 등이 COPPA 규칙에 포함된 것과 동일하거나 그 이상의 기준을 적용한 자율규제 가이드라인의 승인을 FTC에 요청할 수 있도록 한 세이프 하버 프로그램 조항이 포함되어 있음

2019년 2월 2주

또는 온라인상에서 제3자의 아동 개인정보 수집과 관련해 연간 단위로 내부 평가를 수행한다는 새로운 요구사항이 추가됨¹³

- FTC가 승인한 세이프 하버 프로그램에 참여하는 회사나 조직에 대해서는 대부분의 경우, FTC의 정식 조사 및 법 집행 대신 세이프 하버 지침에 제공된 검토 및 징계 절차를 적용

(2) EU의 「GDPR」 및 관련 가이드라인

▶ EU GDPR은 아동의 동의 관련 규정(제8조)이외에도 법 전반에 걸쳐¹⁴ 아동에 관한 개인정보 보호를 강조¹⁵

- 아동은 개인정보 처리에 따른 위험성과 그 결과 및 본인의 권리를 잘 인지하지 못할 수 있으므로, 아동의 개인정보와 관련하여 특별한 보호가 필요하다는 점에 주목
- GDPR은 특히 SNS와 같은 상업적 인터넷 서비스와 관련해 아동의 개인정보보호 문제에 각별한 관심을 강조
- 만 16세 미만의 아동¹⁶에게 직접 서비스를 제공하는 경우, 부모 등 친권을 보유하는 자(holder of parental responsibility)의 동의를 받을 것을 요구¹⁷
- 영국 ICO는 「GDPR 준비를 위해 기관/기업이 취해야 할 12가지 조치사항(Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now)」¹⁸을 통해 “아동 대상의 서비스 제공을 위해 아동의 개인정보를 수집하는 경우¹⁹, 동의는 입증될 수 있어야 하고, 관련 고지는 아동이 충분히 이해할 수 있는 언어로 작성되어야 함”을 적시
- 한편, 아일랜드 DPC의 Helen Dixon 위원장은 GDPR이 어린이 데이터 보호에 관한 원칙을 제시하고 있지만, 구체적인 방법에 내용은 거의 없다고 지적²⁰

(3) 프랑스 데이터보호법(PROJET DE LOI: relatif à la protection des données personnelles)²¹

▶ 15세의 이상부터는 온라인 서비스와 관련하여 개인정보 처리에 대해 스스로 동의할 수

12 2017년 7월 수정됨

13 <https://www.ftc.gov/news-events/press-releases/2017/07/ftc-approves-modifications-trustes-coppa-safe-harbor-program>

14 제6조제1항(f)호, 전문 제38조 및 제75조, 제40조, 제57조제1항(b)호 등

15 출처: 한국인터넷진흥원, 우리 기업을 위한 GDPR 안내서, 2018

16 GDPR은 '아동'이라는 용어의 정의를 별도로 규정하고 있지 않으며, 각 회원국은 자국의 법률을 통해 친권자 동의를 요하는 아동의 연령 기준을 만 13세 미만 까지 낮추어 규정할 수 있음

17 출처: 한국인터넷진흥원, 우리 기업을 위한 GDPR 안내서, 2018

18 <https://ico.org.uk/media/2014146/gdpr-12-steps-infographic-201705.pdf>

19 영국에서는 13세 미만의 개인을 아동으로 정의하므로, 이들의 개인정보를 합법적으로 처리하기 위해서는 부모 또는 보호자의 동의가 필요

20 <https://www.siliconrepublic.com/enterprise/data-privacy-education-schools-dpc>

21 <http://www.assemblee-nationale.fr/15/ta/tap0113.pdf>

있으나, 15세 미만의 미성년자는 본인과 부모 등 친권을 보유하는 자(holder of parental responsibility)가 공동으로 동의한 경우에만 개인정보 처리가 합법으로 간주됨²²

- 그러나 15세 이상인 경우에도 자녀가 특정 응용 프로그램이나 웹 사이트에 등록하기 위해서는 부모 등 친권을 보유하는 자(holder of parental responsibility)의 동의가 요구되는 등 미성년자의 동의 기준은 구체적 사안에 따라 가변적

(4) EU집행위원회의 「모바일 헬스케어 앱 개발자 대상 개인정보보호 행동지침 (Code of Conduct on privacy for mobile health applications)²³」

- ▶ 개인의 건강 관련 데이터가 포함된 개인정보를 처리하는 모바일 헬스케어 앱의 개발 과정에서 적용해야 할 개인정보보호 원칙 중 아동의 개인정보 처리를 위한 동의 관련 내용을 제시
 - 이 행동지침은 EU 집행위원회가 2016년 6월 7일 유럽 시민들의 모바일 헬스케어 앱의 이용이 증가함에 따라, 모바일 헬스케어 앱의 개인정보보호 문제에 대응하기 위하여 발표
 - 16세 미만의 아동을 대상으로 하거나 16세 미만의 아동이 사용할 가능성이 높은 모바일 앱의 개발자는 부모의 책임 아래 동의가 이루어지거나 승인을 받았는지 확인할 수 있도록 지침을 제시
 - 그러나 EU 회원국별 관련 법규에서 규정하는 아동 또는 미성년자의 정의 및 연령 기준이 서로 다를 수 있으므로 각 국가별 상황을 적용

3. 시사점

- ▶ 아동의 개인정보 수집 및 이용에 대한 동의 과정은 ▲정보주체의 연령을 투명하게 확인할 수 있고 ▲부모 등 친권자의 동의를 구하는 과정이 좀 더 효과적일 수 있는 체계를 확보하는 것이 핵심
 - 동의 가능 연령이 법적으로 명시된 경우에도 미성년자들이 나이를 속이는 등의 편법을 동원해 정보주체의 연령 데이터에 대한 정확성과 무결성을 저해하는 문제에 대응
 - 미성년 자녀가 온라인 사이트에 가입하거나 디지털 서비스를 이용할 때마다 신원을 확인하고 동의를 제공해야하는 부모들의 부담을 경감하기 위한 효율적인 시스템을 모색

22 <https://www.lexology.com/library/detail.aspx?g=10a757e1-9dd9-416b-903b-627736380109>

23 EU 집행위원회는 2016년 6월 7일 유럽 시민들의 모바일 헬스케어 앱의 이용이 증가함에 따라, 모바일 헬스케어 앱의 개인정보보호 문제에 대응하기 위하여 이 행동지침을 발표.
http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16125

2019년 2월 2주

- 이런 가운데, 법제를 통해 제시된 동의 조건에 위배되지 않도록 자동화된 신원 확인 및 동의 플랫폼을 개발함으로써 이러한 문제를 해결하기 위한 노력도 이뤄지고 있음
 - 예컨대 미 NIST(National Institute of Standards and Technology)가 백악관 이니셔티브의 일환으로 온라인 신원 확인 모델 'MTF(Minors Trust Framework)'를 개발
- 한편, 일정연령 이하에 대해서는 확일적으로 본인의 동의가 불가능하도록 하는 기존의 방식 대신 개인정보보호에 대한 연령별 인식 수준 차이를 반영해 전적으로 부모나 친권자의 동의에 의지해 엄격한 보호 기준을 적용해야 하는 연령과 이러한 제약을 완화할 수 있는 연령으로 세분화하는 것도 효과적인 방안이 될 것으로 기대
 - 개인정보처리 동의가 가능한 15세 이상의 아동에 대해서도 이용 서비스의 특성에 따라 부모의 동의를 요구하는 프랑스가 대표적인 사례

Reference

1. FTC, FTC updates COPPA compliance plan for business, 2017.06.21
2. FTC, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, 2017.06
3. JDSUPRA, FTC Updates COPPA Guidance for Businesses, 2017.06.23
4. Lexology, FTC's Updated COPPA Compliance Plan Confirms Applicability to IoT Products, 2017.06.22
5. Lexology, (Connected) Toy Story: The FTC Updates the COPPA Compliance Plan, 2017.07.12
6. Silicon Republic, Irish DPC pilots data privacy lessons in Irish schools, 2018.10.16
7. 한국인터넷진흥원, 우리 기업을 위한 GDPR 안내서, 2018



발행일 2019년 2월

발행 및 편집 한국인터넷진흥원 개인정보보호본부 개인정보기획팀

주소 전라남도 나주시 진흥길 9 빛가람동 (301-2) Tel 1544-5118

- ▶ 본 동향보고서의 내용은 한국인터넷진흥원의 공식적인 입장과는 다를 수 있습니다.
- ▶ 해외 개인정보보호 동향보고서의 내용은 무단 전재할 수 없으며, 인용할 경우 그 출처를 반드시 명시하여야 합니다.