GDPR에서 양립성 평가의 판단기준과 적용사례
: 국내법과의 비교·분석을 중심으로

이 창 범*

개정 개인정보 보호법 중 양립성 규정은 가명정보와 더불어 개인정보의 활용 환경을 유연하게 해 줄 수 있는 제도로 산업계로부터 큰 환영과 기대를 받고 있다. 그런데 국내에는 양립성 규정의 배경, 해석, 적용 등에 대한 연구자료가 전무하여 산업계는 물론 감독당국도 법의 해석 및 적용에 대해서 명확한 입장을 내놓고 있지 못하다. 이에 산업계에서는 양립성을 폭넓게 인정받는 방향으로 해석하고 싶어하지만, 감독당국은 매우 조심스럽고 신중한 입장이다. 사실, 개정 개인정보 보호법 및 신용정보법의 양립성 규정은 오남용 가능성과 유명무실한 조항으로 전락할 가능성을 함께 지니고 있다. 국내법상 양립성 규정은 GDPR 제6조제4항을 벤치마킹한 것이나 드러나지 않은 차이점이 적지 않다. 이에 본고는 양립성 규정의 해석 및 적용에 대해서 오랜 경험을 가지고 있는 유럽연합의 사례를 분석해 봄으로써 그와 같은 차이점이 국내법에 미치는 함의와 시사점을 도출해 보고 바람직한 입법 및 해석의 방향을 제시하고자 한다.

주제어: 양립성, 추가처리, 목적외 이용, 개인정보, 가명정보, 오픈데이터, 빅데이터, 공공정보, GDPR

* 연세대학교 법무대학원 겸임교수, 010-9006-4212, miso4all@naver.com

2020/4/30

목 차

Ⅰ. 들어가는 글

2020년 2월 4일 개정된 개정 개인정보 보호법의 가장 큰 특징 중 하나는 양립성 규정의 도입이라고 할 수 있다(제15조제3항 및 제17조제4항).[1] 양립성은 가명정보와 함께 개인정보의 활용 환경을 유연하게 해 줄 수 있는 제도적 장치로 산업계로부터 큰 환영과

1) 개인정보 보호법과 신용정보법은 둘다 "양립성"이라는 용어를 사용하고 있지 않다. 다만, 해당 규정이 GDPR의 양립성 규정(제6조제4항)에 상응하는 것이어서 국내에서도 일반적으로 양립성이라는 용어를 사용하고 있다.

기대를 받고 있다. 가명정보와 양립성은 둘 다 정보주체의 동의없이 개인정보를 활용할 수 있다는 점에서는 같지만, 가명정보는 활용의 범위가 통계작성, 과학적 연구, 공익적 기록보존 등으로 한정된 반면, 양립성은 특별히 활용 범위에 대한 제한이 없고 반드시 가명처리나 익명처리를 해야 하는 것도 아니어서 양자에 대한 기대가 다르다.

예컨대, 양립성 규정에 의할 경우 가명정보의 활용범위를 통계작성, 과학적 연구, 공익적 기록 목적 외에 다른 목적으로 이용할 수 있는 폭넓은 기회를 제공하고, 지금까지 정보주체의 동의를 받지 않으면 목적외 이용·제공이 불가능했던 계약 체결 및 이행과 개인정보처리자의 정당한 이익 추구를 위한 목적외 이용·제공이 가능해지며, 마케팅 목적의 개인정보 이용도 제한된 범위 내에서 가능하게 된다.[2)]

그런데 가명처리 또는 가명화에 대해서는 국내외 관련 연구자료가 많고 이미 관련 서비스를 제공하는 업체들도 많아서 이해의 폭이 비교적 넓으나, 양립성에 대해서는 관련 연구자료나 보고서가 많지 않고 특히 국내에는 양립성 규정의 배경, 해석, 적용 등에 대한 연구·분석 자료가 전무하여 산업계는 물론 규제당국도 그 내용 파악이 싶지 않은 것으로 보인다. 이에 따라 산업계에서는 양립성을 가능한 폭넓게 인정받고 싶어 하지만 규제당국은 매우 조심스럽고 신중한 입장이다.

사실, 개정 개인정보 보호법 제15조제3항 및 제17조제4항과 입법예고 중인 동법 시행령 개정안[3)]만으로는 실무적으로 양립성 규정을 어떻게 적용해야 할지 알기 어렵다. 특히

2) 예컨대, 프로파일링을 통한 맞춤형 광고는 일반적으로 허용되지 않으나 사생활침해 위험이 낮은 공개 알고리즘을 이용한 맞춤형 광고, 거래관계가 있는 정보주체에 대한 동종.유사 제품의 광고성 정보 전송, 로그인이 필요한 금융앱 내에서의 이벤트 행사 등은 양립성 평가를 통해 추가처리가 가능할 수 있다.

3) 제14조의2(개인정보의 추가적인 이용·제공 기준 등) 법 제15조제3항 및 법 제17조제4항에서 "대통령령으로 정하는 바"란 다음 각 호의 사항을 모두 충족하는 경우를 말한다. 이 경우 법 제17조제4항에 관하여는 '이용'을 '제공'으로 본다.

1. 개인정보를 추가적으로 이용하려는 목적이 당초 수집 목적과 상당한 관련성이 있을 것
2. 개인정보를 수집한 정황과 처리 관행에 비추어 볼 때 추가적으로 이용할 수 있을 것으로 예측 가능할 것
3. 개인정보의 추가적 이용이 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니할 것
4. 가명처리를 하여도 추가적 이용 목적을 달성할 수 있는 경우에는 가명처리하여 이용할 것

「신용정보의 이용 및 보호에 관한 법률」(이하 "신용정보법"이라 한다) 제32조제6항제9의4호[4]는 GDPR과 법률의 체계나 규율 방식이 많이 다름에도 불구하고 GDPR 규정을 그대로 번역해 놓은 듯하여 법의 해석 및 적용이 더욱 막막할 것으로 보인다. 이에 따라 현행 양립성 규정은 오남용 가능성과 유명무실한 조항으로 전락할 가능성을 함께 지니고 있다고 할 수 있다.

본고는 양립성 규정의 적용과 관련해 오랜 경험을 가지고 있는 유럽연합의 사례 분석을 통해 양립성 규정이 나아가야 할 해석의 방향을 제시하고자 하는데 목적이 있다. 또한, 국내법상 양립성 규정은 GDPR 제6조제4항을 벤치마킹한 것이나 자세히 살펴보면 숨어 있는 차이가 적지 아니한 바 그와 같은 차이가 국내법에 어떤 의미를 시사하는지에 대해서도 살펴보고자 한다.

Ⅱ. 양립성 및 추가처리의 의미와 의의

1. 양립성의 의미와 의의

양립성 또는 양립가능성(compatibility)이란 개인정보를 추가적으로 처리하고자 하는 목적이 당초 수집시의 처리 목적과 양립할 수 없는 것이 아니라면—다시 말해 서로 상충하지 않는다면— "목적제한원칙"에 어긋나지 아니한 것으로 보아 추가 목적의 개인정보 처리에 대해서 정보주체의 동의를 받지 않아도 된다는 것이다. 이 때문에 양립성 규정을

4) 제32조(개인신용정보의 제공·활용에 대한 동의) ⑥ 신용정보회사등(제9호의3을 적용하는 경우에는 데이터전문기관을 포함한다)이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다.
9의4. 다음 각 목의 요소를 고려하여 당초 수집한 목적과 상충되지 아니하는 목적으로 개인신용정보를 제공하는 경우
가. 양 목적 간의 관련성
나. 신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경위
다. 해당 개인신용정보의 제공이 신용정보주체에게 미치는 영향
라. 해당 개인신용정보에 대하여 가명처리를 하는 등 신용정보의 보안대책을 적절히 시행하였는지 여부

GDPR 제6조제1항에서 규정하고 있는 적법처리의 근거에 추가하여 독립적인 처리의 근거로 보려는 견해도 있다.[5] "목적제한원칙"이란 개인정보를 수집할 때에는 처음부터 ① 개인정보의 처리 목적을 구체적이고 명시적으로 제시해야 하고, ② 합법적인 목적을 위해서 수집해야 하며, ③ 최초 수집 목적과 양립(부합)하지 않는 방식으로 추가처리를 해서는 않는다는 원칙이다.[6]

"목적제한원칙"은 개인정보의 수집 이유를 구체적이고 명확하게 고지·공개함으로써 개인정보의 처리 활동이 정보주체의 합리적인 기대와 일치하도록 하게 하는 것을 목적으로 한다. 이를 통해 개인정보처리에 대한 정보주체의 신뢰를 확보하고자 하는 것이다. 처음부터 처리 목적을 명확히 해두면 개인정보처리에 대한 개인정보처리자의 책임감을 높이고 개인정보처리자가 은연중에 처리 목적을 확대하는 것을 막을 수 있다. 또한 정보주체는 개인정보처리자가 개인정보를 어떻게 이용할지 이해할 수 있고, 개인정보처리에 대한 동의의 선택 등 정보주체의 권리 행사에도 도움을 준다.

그런데 빠른 기술발전과 사회변화에 따라 개인정보처리자의 개인정보처리 환경은 계속해서 변하고 정보주체의 기대도 환경 변화와 함께 변한다. 그럼에도 불구하고 목적제한원칙에 어긋난다는 이유로 수집시 예상할 수 없었던 모든 목적외의 개인정보처리를 엄격히 금지한다면 경제·사회 발전에 역행하는 결과를 초래하게 된다. 양립성은 이와 같은 상황에서 경제·사회의 현실적이고 합리적인 요구를 수용함으로써 개인정보처리자가 일정한 범위 내에서 정보주체의 추가적인 동의나 입법적 조치 없이 개인정보를 처리할 수 있는 융통성을 제공해 준다.

---

5) Monica Iancu & Vasile Soltan(February 10 2020), Compatibility of purpose for further processing of personal data: hit the bull's eye in darts or hit the ball in a rugby gate? p.2

6) GDPR은 개인정보처리를 위한 일반원칙으로 ① 적법성(lawfulness), ② 공정성(fairness), ③ 투명성(transparency), ④ 목적제한(purpose limitation) ⑤ 최소처리(data minimisation), ⑥ 정확성(accuracy), ⑦ 보관제한(storage limitation), ⑧ 보안성(integrity and confidentiality). ⑨ 책임성(accountability) 등 9가지를 제시하고 있다(제5조). 이와 같은 원칙 중 하나를 위반한 것만으로도 개인정보처리자 또는 수탁자에게는 전세계 매출액의 4% 또는 2천만 유로 중 더 많은 금액의 과징금(administrative fines)이 부과될 수 있다(제83조제5항).

2. 추가처리의 의미와 목적외 이용과의 차이

양립성 평가[7]에서 개인정보의 "추가처리(further processing)"란 최초 수집시의 목적을 위한 처리인지 그 이후 새롭게 정의된 목적을 위한 처리인지 여부를 불문하고, 최초 수집 활동 이외의 모든 처리 활동을 통틀어서 추가처리라고 한다.[8] 다시 말해 추가처리란 개인정보의 수집 행위 이외의 모든 처리활동(이용, 제공, 저장, 가공, 편집, 삭제, 결합 등의 모든 활동)을 의미한다. 따라서 최초 수집 행위 이외의 모든 처리 활동은 원칙적으로 양립성 요건을 충족하여야 한다.[9] 다만, 추가처리는 최초 수집한 개인정보의 존재를 전제로 하므로 새로운 개인정보의 "수집"은 양립성 평가에 의한 추가처리의 대상으로 보기 어렵다.

GDPR 상 추가처리를 위한 가장 일반적인 방법으로는 i) 새로운 목적에 대하여 정보주체의 구체적·명시적인 동의를 받는 것, ii) 새로운 처리에 대해서 양립성 평가를 하는 것, iii) 민주사회에 있어서 필요하고도 비례적인 조치가 갖추어진 법률을 제·개정하는 것이다.[10] 정보주체의 동의를 받거나 법률을 제·개정하는 것은 절차가 어렵고 힘들기는 하지만 그 수단과 범위가 명확해서 분쟁의 소지가 적은 반면, 양립성 평가는 자체적인 판단으로 적용할 수 있어 편리하지만 양립성의 판단기준이 추상적이어서 법적 제재를 받거나 분쟁의 대상이 될 수 있다.[11] 이에 따라 후술하는 사례 분석에서 본 바와 같이 GDPR의 전신인 Directive 시절에도 매우 치밀하고 엄격한 평가를 실시하고 있다.

---

7) 후술하는 바와 같이 GDPR에서도 양립성 평가라는 용어를 사용하고 있지는 않다. "확인" 또는 "고려"라는 용어를 사용하고 있을 뿐이다. 다만, 확인 또는 고려를 체계적으로 수행해야 한다는 의미에서 EU에서는 실무적으로 양립성 평가라는 용어가 광범위하게 사용되고 있다. 본고에서도 양립성 평가란 양립성 고려의 절차와 방법을 의미하는 것으로 사용한다.

8) 29WP(2013), Opinion on Purpose Limitation, p.21

9) 29WP, 앞의 의견서, p.21

10) GDPR 제6조제4항 본문 ; Monica Iancu & Vasile Soltan, p.2 ; Wouter Seinen, Andre Walter & Sari van Grondelle, Compatibility as a Mechanism for Responsible Further Processing of Personal Data, pp.2-3.

11) 개인정보 추가처리에 대한 동의와 양립성의 장단점, 적용규정 등의 차이에 대해서는 Wouter Seinen, Andre Walter & Sari van Grondelle, 앞의글 참조.

우리나라 개인정보 보호법도 GDPR의 추가처리에 상응하는 개념으로 제15조제2항·제17조제2항·제18조제3항의 변경 동의 규정과 제18조제2항의 목적외 이용·제공 규정에 추가하여 제15조제3항 및 제17조제4항의 양립성 규정까지 신설함으로써 GDPR 체계에 맞추려고 노력하고 있다. 그러나 GDPR에서 양립성 평가를 통해서 처리할 수 있는 "추가처리"의 범위와 개인정보 보호법 제15조제3항 및 제17조제4항의 양립성 규정에 의해서 처리할 수 있는 "추가처리"의 범위는 반드시 일치하지 않다. 앞에서 살펴본 바와 같이 GDPR 제6조제4항에 의한 추가처리에는 최초의 수집 행위 이외의 모든 것이 포함되는 반면, 개인정보 보호법 제15조제3항 및 제17조제4항에 따른 추가처리의 범위 또는 대상은 명확하지 않다.

즉, 개인정보 보호법 제15조제3항 및 제17조제4항은 '당초 수집 목적과 합리적으로 관련된 범위에서 이용 또는 제공할 수 있다'고 규정함으로써 합리적인 범위 내에서 수집한 개인정보를 "이용" 또는 "제공"할 수 있는 것은 분명하지만, 개인정보의 이용·제공·보관 기간은 언제까지 가능한지, 이용하거나 제공하는 개인정보의 항목도 추가 및 확대가 가능한지, 개인정보를 제공받는 자의 추가 및 확대도 가능한지 여부 등은 불분명하다.

생각건대, 양립성은 양립하지 않는 경우를 제외하고 가능하면 추가처리를 유연하게 인정하고자 하는 것이므로 양립성 제도의 취지를 고려할 때 개인정보의 처리 기간, 항목, 제공받는 자에 대해서도 "합리적으로 관련된 범위 내"에서 연장 및 확대가 가능하다고 보아야 할 것이다.[12] 다만, 개인정보 보호법상으로도 "당초 수집 목적과 합리적으로 관련된 범위에서"만 이용 또는 제공이 가능하므로 새로운 개인정보의 "수집"은 불가능하다고 보아야 한다.

12) 다만, 제3자 제공시 수령인의 범위를 범주(category)로 고지·공개하는 것을 허용하고 있는 GDPR과 달리 수령인의 이름을 명시하고 구체적인 이용·보관 기간을 특정하도록 요구하고 있는 국내법 현실에서 이와 같은 해석이 가능할지는 좀더 검토가 필요하다.

Ⅲ. 양립성 평가를 통해 추가처리가 가능한 개인정보의 범위

1. 일반 개인정보의 추가처리

원칙적으로 GDPR 제5조(개인정보의 처리원칙)[13] 및 제6조제1항(개인정보의 적법처리기준)에 따라 적법하게 수집된 개인정보는 추가처리의 대상이 될 수 있다. 바꿔 말해, GDPR 제5조 및 제6조제1항을 위반하여 불공정하거나 불법적으로 수집한 개인정보는 추가처리의 대상이 될 수 없다. GDPR은 개인정보의 적법처리의 근거로 1) 정보주체의 명시적 동의, 2) 정보주체와 체결한 계약이행, 3) 법률상의 의무준수, 4) 정보주체 또는 자연인의 중대한 이익보호, 5) 공적 업무수행 또는 권한행사, 6) 개인정보처리자 또는 제3자의 정당한 이익 추구를 규정하고 있다. 이상의 여섯 가지 적법처리 요건 중 하나를 충족하고 제5조의 개인정보처리원칙을 모두 충족해야 적법한 처리로 인정받는다.

그러나 제5조 및 제6조제1항의 적법처리의 요건을 갖추었다고 해서 모든 개인정보에 대해서 양립성 규정을 적용해 추가처리를 할 수 있는 것은 아니다. “양립성 평가”에 의해서 추가처리를 할 수 있는 개인정보는 최초의 수집 근거가 2) 정보주체와 체결한 계약이행, 4) 정보주체 또는 자연인의 중대한 이익보호, 6) 개인정보처리자 또는 제3자의 정당한 이익 추구에 해당하는 경우에 한해서 인정된다. 최초의 개인정보 수집 근거가 1) 정보주체의 명시적 동의, 3) 법률상의 의무준수, 5) 공적 업무수행 또는 권한행사를 위한 목적인 경우에는 양립성 평가를 통한 개인정보의 추가처리는 인정되지 않는다.[14]

따라서 “동의”를 기반으로 개인정보를 수집한 경우에는 새로운 처리가 공정하고 합법적인 것임을 보장하기 위하여 새로운 동의를 받아야 하고, 법률상 규정에 의해서 수집된 것

---

13) 각주 6) 참조

14) GDPR 제6조제4항 본문; An official EU website, [Q&A] Can we use data for another purpose? 공식 사이트는 개인정보처리가 정당한 이익(legitimate interest), 계약 체결 및 이익(contract), 중대한 이익보호(vital interests)에 근거한 경우에 한해 양립성이 허용되고 동의(consent)나 법적 요구(legal requirement)에 근거한 경우에는 추가처리가 허용되지 않음을 명확히 밝히고 있다. ; 이론적 배경은 WP29, Guidelines on Consent under Regulation 2016/679, 10 April 2018, p.23 참조.

이라면 법률의 개정에 의해서만 추가처리가 가능하다. 정보주체의 동의에 근거해서 수집한 개인정보에 대해서 양립성 평가를 적용하여 추가처리를 허용할 경우 동의에 대한 정보주체의 신뢰를 훼손할 수 있고, 법률의 규정에 근거해 수집한 개인정보에 대해 양립성 평가를 인정할 경우 법치행정의 정신에 반할 수 있기 때문이다.[15)]

GDPR과 달리 우리나라 개인정보 보호법은 정보주체의 동의에 의해서 수집한 개인정보와 법령에 근거해서 수집한 개인정보는 추가처리의 대상이 될 수 없다는 내용을 명시하고 있지 않다. 따라서 정보주체의 동의 또는 법령에 근거해서 수집한 개인정보도 원칙적으로 추가처리의 대상이 될 수 있다(제15조제3항, 제17조제4항). 신용정보법도 양립성 규정을 적용하여 추가처리를 할 수 있는 개인정보의 대상에 대하여 특별한 제한을 두고 있지 않다(제32조제6항제9의4호, 제33조제1항제4호).

다만, 국내의 경우에도 양립성 평가의 고려 요건으로 개인정보의 수집정황(또는 수집경위), 추가처리의 예상 가능성 등을 고려하도록 규정하고 있으므로 정보주체의 동의 또는 법령의 규정에 근거해서 수집한 개인정보는 양립성 요건을 충족할 가능성이 낮다는 이유로 양립성을 부정하는 해석이 나올 가능성도 없지 않다. 그러나 국내의 경우 동의의 예외사유에 대한 해석이 엄격하고, 정보통신서비스 제공시에는 사실상 동의를 적법처리의 원

15) 이 경우 다른 법률이란 GDPR 제23조에 따른 법률을 의미한다. GDPR 제23조는 국가안보, 국방, 공공안전, 범죄의 예방·수사·적발·기소 및 형의 집행, EU 또는 회원국의 중요한 공익의 보호(특히 통화·예산·조세·공중보건·사회보장 등을 포함한 경제적·재정적 이익), 사법적 독립 및 절차의 보호, 규제받는 전문직에 적용되는 윤리위반의 예방·조사·적발·기소, 공적권한의 행사 및 그와 관련된 감시·검사 및 규제 기능의 수행, 정보주체 또는 다른 사람의 권리와 자유 보호, 민사법상의 청구의 집행을 위하여 필요한 경우 제5조(개인정보의 처리원칙), 제12조에서 제22조(정보주체의 권리), 제34조(개인정보 침해통지)의 의무와 권리를 제한할 수 있는 입법적 조치를 취할 수 있도록 개인정보처리원칙에 대한 예외를 규정하고 있다. 다만, 이 경우 예외적인 입법적 조치는 의무와 권리의 제한이 기본권과 자유의 본질을 존중하여야 하고, 민주사회에서 공익을 보호하기 위해 필요하고도 비례적이어야 하며, 최소한 개인정보의 처리 목적, 처리될 개인정보의 범주, 오남용 방지장치, 구체적인 컨트롤러 및 프로세서, 개인정보의 보관기간, 적용가능한 안전장치, 정보주체의 권리에 미치는 위험, 정보주체의 고지받은 권리 등을 포함하고 있어야 한다. 이와 달리 우리나라 개인정보 보호법 제58조는 국가안보, 공중보건 등 공익 목적을 위하여 필요한 경우 개인정보 보호법의 적용을 포괄적으로 면제하고 있고 별도의 입법적 조치를 요구하고 있지 아니하며 별도 입법적 조치의 기준도 제시하고 있지 않다.

칙으로 삼고 있어 GDPR과 같이 동의에 근거해서 수집한 개인정보에 대해서 양립성 규정의 적용을 배제할 경우 양립성 규정의 효용성은 반감할 것이다.

2. 민감정보 등의 추가처리

GDPR에서는 민감정보, 범죄정보, 고유식별정보 등도 적법하게 수집된 것이라면 원칙적으로 추가처리의 대상이 될 수 있다. 그러나 민감정보, 범죄정보, 고유식별정보 등은 그 밖의 "민감성 정보"와 함께 사생활 침해 가능성이 높기 때문에 양립성 평가시 중요한 고려요소 중 하나가 되며, 따라서 GDPR에서도 양립성 평가를 통해서는 사실상 추가처리가 제한된다.

이에 반해, 우리나라 개인정보 보호법은 민감정보, 고유식별정보 및 공개된 장소에서 수집된 개인영상정보를 양립성 원칙의 적용 대상에서 배제하고 있는 것으로 볼 수 있다. 개인정보 보호법은 "양립성 원칙"을 제15조와 제17조에서만 규정하고 있고, 제23조(민감정보의 처리 제한), 제24조(고유식별정보의 처리 제한) 및 제25조(영상정보처리기기의 설치·운영 제한)에서는 규정하고 있지 않기 때문이다.[16]

3. 가명정보의 추가처리

GDPR에서 가명처리는 암호화 등과 함께 개인정보를 안전하게 활용 및 보관하기 위한 안전조치 중 하나이며 양립성 평가시 5대 고려요소 중 하나이기도 하다. 우리나라와 달리 GDPR에서는 가명정보의 처리 목적이 특별히 제한되어 있지 않다. 즉, 개인정보처리자는 GDPR 제6조제1항 각 호의 적법처리요건 중 어느 하나에 해당하면 개인정보를 안전하게 처리하기 위해서 언제든지 가명조치하여 처리할 수 있다. 더 나아가, GDPR 제89조제1항에 따라 가명정보를 공익적 기록, 역사적, 과학적 및 통계적 목적으로 추가처리하는 경우에는 최초의 목적과 양립 가능한 것으로 간주된다(제5조제1항(b)).

16) 이에 대해서는 개인정보 보호법 제15조제3항 및 제17조제4항을 일반규정으로 보아 제23조, 제24조, 제25조에 대해서도 적용이 가능하다는 해석이 있을 수도 있다.

GDPR 제89조제1항은 공익적 기록, 역사적, 과학적 및 통계적 목적으로 개인정보를 처리할 때에는 개인정보 최소처리 원칙을 보장하기 위한 기술적·관리적 조치를 포함하여 정보주체의 권리와 자유를 보호하기 위한 적절한 안전조치를 적용하여야 한다고 규정하면서, 그와 같은 안전조치에는 가명처리도 포함될 수 있다고 규정하고 있다. 그러나 가명처리를 했다고 해서 무조건 양립성이 간주되는 것은 아니다. 양립성을 인정받기 위해서는 적절한 안전조치를 해야 하는데 정보주체의 권리와 자유를 보호하기 위한 적절한 방식으로 가명처리를 해야 하고[17] 목적을 충족할 수 있는 한 정보주체의 식별을 더 이상 허용하지 않도록 조치해야 한다(제89조제1항 후단).

적절한 방식으로 가명처리가 된 가명정보를 공익적 기록, 역사적, 과학적 및 통계적 목적으로 처리하는 한 최초의 수집 목적과 양립 가능한 것으로 간주되지만, 그 밖의 목적으로 가명정보를 추가처리하기 위해서는 case by case로 양립성 여부를 평가해야 한다. 가명정보를 공익적 기록, 역사적, 과학적 및 통계적 목적으로 처리하는 경우에는 양립성이 간주되므로 이 경우에는 정보주체의 동의 또는 법률의 특별한 규정에 의해서 수집된 개인정보도 추가처리를 할 수 있다.

4. 계약 체결·이행 및 정당한 이익 추구를 위한 추가처리

개인정보 보호법 제17조제1항은 제15조제1항과 달리 1)정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우, 2)개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우에도 정보주체의 동의를 받지 않으면 개인정보를 제공할 수 없게 하고 있다. 그런데 제17조제4항의 신설로 인

17) GDPR에서는 가명조치가 개인정보를 안전하게 처리하기 위한 보호수단에 불과하다. 개인정보를 원래 목적 범위 내에서 안전하게 처리하기 위하여 가명조치를 할 때는 직접식별자(고유식별자)만 비식별조치를 해도 되지만 다른 목적으로 이용 또는 제공하고자 하는 경우에는 간접식별자(준식별자), 특이정보, 속성정보 등까지 비식별조치를 해야 할 경우도 있다. 가명정보 또는 가명처리에 대한 자세한 설명은 KISA REPORT 2020 vol.5(한국인터넷진흥원, 2020.5)에 발간 예정인 졸고 「가명정보에 있어서 '다른 정보'와 '추가 정보'의 차이 및 가명처리의 대상과 범위」를 참고

해 이와 같은 경우에도 양립성 평가를 통해 추가처리를 할 수 있는 길이 열렸다고 할 수 있다. 계약의 체결 및 이행을 위해 필요하거나 정당한 이익 추구를 위한 것이므로 목적 관련성을 인정받기 쉽고 합리적으로 예측이 가능하며 정보주체에게 예상치 못한 불이익을 줄 가능성도 낮기 때문이다. 따라서 개인정보를 수집한 정황이 불공정 또는 불공평하지만 않다면 양립성을 인정할 수 있을 것이다.

하지만, 개인정보 보호법 제18조는 동조 제2항에서 열거한 경우를 제외하고 일체의 목적외 이용과 제공을 금지하고 있다. 이에 따라 제17조제4항과 제18조의 관계가 불분명한 관계가 되고 있다. 즉, 제17조제4항은 제18조의 제한 범위 내에서만 추가처리가 가능하다고 보아야 할지(제15조 및 제17조와 달리 제18조에는 양립성 규정을 두고 있지 않음), 제17조제4항이 제18조에 우선하여 적용된다고 보아야 할지 여부가 불분명하다. 제18조의 제한 범위 내에서만 제17조제4항에 따른 추가처리가 가능하다고 하면 제17조제4항의 효용성이 크게 감소할 것이고 제15조제3항에 따른 추가처리도 제18조의 제한 범위 내에서만 이용이 가능하다고 하게 되어 매우 불합리한 결과가 된다.

따라서 개인정보처리자는 제18조의 제한 규정에도 불구하고 신법우선원칙에 따라 또는 특별규정우선원칙에 따라 제15조제3항 및 제17조제4항에 근거하여 '계약 체결 및 이행' 또는 '정당한 이익추구'에 대해서도 양립성 규정을 적용하여 추가처리가 가능하다고 하여야 할 것이다. 개인정보 보호법 제15조제3항 및 제17조제4항에 양립성 규정이 신설되기 전에는 제18조가 제한된 범위 내에서 GDPR의 양립성 규정과 같은 적극적인 역할을 수행해 왔으나 양립성 규정의 신설로 제18조제2항의 역할과 기능에 대한 새로운 검토가 필요하게 되었다.

Ⅳ. 양립성 평가의 절차 및 방법

1. 양립성 평가의 필요성 판단

개인정보처리자가 수집시의 목적과 다른 목적으로 개인정보를 처리하기 위해서는 정보주체의 동의를 받거나 양립성을 입증해야 한다. 그러나 추가처리가 필요하다고 해서 모든 경우에 있어서 정보주체의 “동의”를 받거나 양립성 평가를 해야 하는 것은 아니다. 정보주체가 합리적으로 기대할 수 있는 범위 내의 추가처리라서 양립성이 명백하다면(prima facie obvious) 양립성 평가는 필요하지 않을 수 있다.[18] 따라서 개인정보처리자는 양립성 평가에 앞서 해당 추가처리가 양립성 평가를 필요로 하는 것인지 여부부터 확인해야 한다.

기술이나 서비스의 변화에 따라 개인정보의 추가처리에 대한 사회일반 또는 정보주체 자신의 기대가 변화할 수 있는 환경에서 추가처리의 범위에 대해서도 보다 유연한 접근방법이 필요하다. 개인정보를 수집할 당시에는 개인정보처리자와 정보주체 둘 다 추가처리가 필요하지 않다고 생각했을 수 있지만, 추후 상황의 변화에 따라 다른 목적으로 처리하는 것이 유용할 수 있는 경우가 얼마든지 있을 수 있다.[19]

최초 수집시 필요한 목적이 구체화되어 있고 그 목적 달성을 위해 필요한 범위 내의 개인정보가 관례적인 방식으로 처리되고 있어서 정보주체가 그와 같은 처리를 합리적으로 충분히 예상할 수 있는 경우라면 수집시 모든 조건(details)을 다 충족하지 못했더라도 양립성 평가는 필요하지 않을 수 있다. 예컨대 매주 1회 집으로 야채를 배달해 주기로 계약을 체결하고 야채 배달 및 결제 목적으로 최초 수집한 개인정보를 매주 반복해서 이용하는 경우 미리 반복 이용에 대해서 정보주체에게 명시적으로 고지하지 않았더라도 추가처리는 최소 수집 목적 달성을 위해 논리적으로 당연히 요구되는 것이므로 반복 이용에 대해서 굳이 양립성 평가를 거칠 필요가 없다.[20]

---

18) 29WP, 앞의 의견서, p.22
19) 29WP, 앞의 의견서, p.21
20) 29WP, 앞의 의견서, p.22

반면, 양립성 여부가 명확하지 않거나(애매하거나) 합리적인 사람이 예상하기 어려운 추가처리라면 반드시 양립성 평가를 해야 한다. 처리 목적이 수집시 목적과 관련성은 있으나 완전히 일치하지 않는 경우 또는 간접적으로만 관련성이 있는 경우 등도 마찬가지이다. 특히 합리적인 사람이라면 반대할 수도 있는 정도의 추가처리에 대해서는 보다 엄격한 평가가 필요하다. 수집시 명시된 초기 목적과 추가 목적 사이의 거리가 멀수록 평가는 보다 더 철저해야 하고 정보주체의 이익을 보호하기 위한 추가적인 보호조치가 요구된다. 예컨대, 야채 배달 목적으로 수집하거나 생성한 개인정보를 자사가 판매하고 있는 다른 유사 유기농 상품의 광고·홍보 목적으로 이용하고자 할 때(할인쿠폰 등의 제공)에는 소비자마다 생각이 다를 수 있으므로 양립성 평가가 필요하다.[21]

2. 양립성 평가의 절차 및 방법

GDPR은 개인정보의 추가처리가 정보주체의 동의나 법률의 규정에 의한 경우를 제외하고 '최소 수집시의 목적과 양립하는지 여부를 확인(ascertain)하기 위하여 다음 각호의 사항을 고려하여야 한다'라고만 규정하고 있을 뿐 평가(assessment or test)를 해야 한다거나 평가 방법을 제시하고 있지는 않다. 따라서 GDPR에는 양립성 평가를 위한 어떤 체계화된 절차나 방법이 마련되어 있지 않다. 우리나라 개인정보 보호법도 양립성 평가를 위한 절차 및 방법에 대해서는 규율하고 있지 않다. 보다 엄밀하게 말해서 국내법에서는 양립성이라는 용어도 사용하고 있지 않다.

그럼에도 불구하고 WP29(2013)는 공식 의견서에 양립성 평가라는 용어를 사용하고 있고 양립성 평가의 방법에 대해서 기술하고 있다. 개인정보처리자는 추가처리와 관련하여 분쟁이 발생하거나 감독기관의 조사에 직면해야 할 경우도 있을 수 있으므로 양립성 평가와 관련해서는 WP29의 제안을 고려하지 않을 수 없을 것이다.[22] WP29는 양립성 평가의 방법에 따라 감독당국의 결론이 달라질 수 있음을 인식하면서 양립성은 실질적인

21) 29WP, 앞의 의견서, pp.22-23
22) Wouter Seinen, Andre Walter & Sari van Grondelle, 앞의 글, p.4

방식으로 평가해야 한다는 점을 강조하고 있다.[23]

"실질적 평가"란 개인정보가 수집된 정황을 포함해 관련 상황과 요소들을 종합적으로 고려해 문서로 제시된 목적을 넘어 실질적으로 비교·평가하는 것이다.[24] 실질적 평가는 유연하고 실용적이고 효과적이며 미래 사회의 발전에 적응할 수 있게 해 줄 뿐 아니라 동시에 정보주체의 개인정보를 계속해서 효과적으로 보호하는 것에 보다 신경을 쓰도록 유도해 준다. 이에 반해, "형식적 평가"란 개인정보처리자가 최초로 개인정보를 수집할 때 문서로 제시한 목적과 추가 목적을 자구에 충실하게 형식적으로 비교·평가하는 방식이다. 형식적 평가는 외견상으로는 객관적이고 중립적인 것으로 보일 수 있으나 평가가 너무 엄격하고 자구에 집착하게 되어 개인정보처리자로 하여금 정보주체를 보호하는데 신경을 쓰게 하기 보다는 추가처리의 범위를 확대할 수 있는 묘안(목적의 느슨화)을 궁리하는데 신경을 쓰게 할 우려가 있다.

사실, GDPR은 양립성을 설계함에 있어서 추가처리가 최초 수집 목적과 "양립 가능한 것"인지 여부보다는 "양립할 수 없는 것"인지 여부에 대해서 더 초점을 두고 있다. 즉, 양립이 가능한 경우의 요건을 적극적으로 규정하기 보다는 양립이 불가능한 경우(상충하는 경우)에만 추가처리를 금지하는 소극적인 방법을 채택하고 있다.[25] 따라서 최초의 목적과 다르다는 사실만으로 양립성이 필연적으로 또는 자동적으로 배제되지는 않는다.[26] 최초 수집 목적과 양립이 가능한 경우에만 처리할 수 있다는 것과 양립할 수 없는 경우가 아니면 처리할 수 있다는 것은 접근방법에 있어서 차이가 있다. 후자가 전자에 비해서 더 유연성을 부여해 준다. 즉, 양립 가능해야 추가처리가 가능하다고 하면 최초 수집 "목적"과 일치하지 않을 경우 추가처리를 인정할 여지가 좁아지지만, 양립할 수 없는 경우가 아니면 처리할 수 있다고 하면 추가처리를 인정할 여지가 더 커진다.[27]

---

23) 29WP, 앞의 의견서, pp.21-22
24) 29WP, 앞의 의견서, pp.21-22
25) 29WP, 앞의 의견서, p.21. ; Monica Iancu & Vasile Soltan, 앞의 글, p.2 ; Wouter Seinen, Andre Walter & Sari van Grondelle, 앞의 글, p.3.
26) 29WP, 앞의 의견서, p.39
27) 29WP, 앞의 의견서, p.21

예컨대, 금융회사가 신용대출 목적으로 수집한 소비자의 개인정보를 1년 후 소비자에게 더 유리한 다른 대출상품으로 전환하도록 안내하기 위한 목적으로 이용한다고 가정해 보자. 양립이 가능해야만 추가처리가 가능하다고 해석할 경우 대출 목적으로 수집한 개인정보를 대출상품 전환 안내 목적으로 이용하는 것은 최초의 수집 목적과 양립하지 않는다고 볼 수 있다. 이에 반해, 양립할 수 없는 경우가 아니면 추가처리가 가능하다고 해석하면 대출상품 전환 안내 목적의 개인정보 이용은 최초 목적(대출 목적)과 양립할 수 없는 것은 아니라는 결론에 비교적 쉽게 도달할 수 있다.

이에 반해 우리나라 개인정보 보호법은 '당초 수집 목적과 합리적으로 관련된 범위에서' 개인정보를 이용 또는 제공할 수 있다고 명시하고 있어 일단 관련 범위를 벗어나기만 하면 양립성은 필연적으로 또는 자동적으로 배제되는 것으로 해석될 여지가 적지 않다. 따라서 GDPR과 같은 유연한 해석 방법(실질적 평가)을 채택하는 데에는 한계가 있을 것으로 보인다.

3. 고려요소의 적용방법 : 고려요소 간의 관계

개인정보처리자가 양립성 여부를 확인할 때에는 아래의 다섯 가지 고려요소들을 고려해서 판단해야 한다(GDPR 제6조제4항). 아래 고려요소를 종합적으로 고려해 수집시의 목적과 추가처리의 목적이 양립할 수 없는 것이 아니면(상충하지 않으면) 추가처리가 가능하다.

(a) 개인정보의 최초 수집시 목적과 의도된 추가처리 목적 간의 관련성(link);
(b) 개인정보가 수집된 정황(context). 특히 정보주체와 개인정보처리자 간의 관계와 관련된 정황;
(c) 개인정보의 성질(nature), 특히 GDPR 제9조에 따른 특별 범주의 개인정보가 처리되는지 여부 또는 제10조에 따른 범죄와 관련된 개인정보가 처리되는지 여부
(d) 정보주체에게 미칠 수 있는 추가처리의 가능한 결과(possible consequence);
(e) 암호화 또는 가명화를 포함하여 적절한 보호수단(appropriate safeguards)의 존재

개인정보처리자는 (a), (b), (c), (d), (e)의 모든 사항을 종합적으로 고려해서 판단해야 하지만, (a)~(e)는 어디까지나 "복합적 고려사항(multi-factor assessment)"일 뿐 빠짐없이 준수해야 하는 "필수 준수요건"은 아니다.[28] 따라서 (a)~(e)는 하나가 다른 하나의 결함 또는 결점을 보완해 줄 수 있는 상호 보완관계 또는 보충관계가 될 수 있다. 특히 (e)는 독립적으로 요구되는 필수 준수사항이 아니며, (a)~(d)의 부정적 결과를 보완해 주는 보완적·보충적.보상적 관계에 있다.

예컨대, 수집시의 목적과 추가 목적 간에 관련성이 낮아도 정보주체가 추가처리를 충분이 예상할 수 있고 정보주체에게 미치는 영향이 부정적이지 않으며 가명화 등의 보호조치를 취했다면 부족한 목적 관련성은 보완된 것으로 볼 수 있고, 추가처리가 정보주체에게 불이익을 줄 수 있는 경우에도 관련성이 충분하고 예측 가능하며 개인정보의 수집 정황이 공평하고 가명화 등의 보호조치를 취해 불이익을 최소화했다면 추가처리로 인해 정보주체에게 야기될 수 있는 불이익이 상쇄되었으므로 양립성이 인정될 수 있다.

이상의 요소들을 고려해서 양립성 평가를 할 때에는 정보주체의 관점과 개인정보처리자의 관점을 모두 균형있게 고려하여야 한다. 정보주체 측면에서는 추가처리에 대한 정보주체의 기대, 신뢰, 법적 확실성 등을 고려해야 하고, 개인정보처리자 측면에서는 수집 시에는 제시하지 않았던 추가처리의 목적이 혁신, 경쟁 및 마케팅 발전에 진정으로 기여하는 것인지 여부를 고려해야 한다.[29]

우리나라 개인정보 보호법도 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하도록 규정함으로써 양립성 판단기준을 "고려사항"으로 규정하고 있으나(제15조제3항, 제17조제4항), 현재 입법 예고 중인 시행령 개정안은 양립성 판단기준을 모두 충족한 경우에만 추가처리가 가능하다고 규정함으로써 사실상 고려요소가 아닌 필수 준수요건으로 전환시키고 있다(시행령 개정안 제14조의2).

---

28) 29WP, 앞의 의견서, p.27

29) Monica Iancu & Vasile Soltan, 앞의 글, p.2

Ⅴ. 양립성 평가시 5대 고려요소

1. 개인정보의 수집시 목적과 추가처리 목적의 관련성(link)

개인정보처리자는 수집시의 처리 목적과 추가처리의 목적 간의 관계(link or relationship)를 검토해야 한다. 최초 수집시의 처리 목적에 추가처리가 암묵적으로 포함되어 있을 수 있고, 수집시 처리 목적과 부분적으로 관련이 있을 수도 있다. 또한, 형식상으로는 관련이 없는 것처럼 보이지만 논리적으로 추가처리가 다음 단계로 간주되는 상황도 존재할 수 있다. 이런 경우에는 비교적 양립성을 쉽게 인정할 수 있을 것이다. 일반적으로 수집시의 처리 목적과 추가처리 사이의 거리가 멀수록 양립성 평가는 불리해진다.

수집시 목적과 추가처리의 관계를 분석할 때에는 최초 수집시의 목적을 문자 그대로만 파악해서는 안 되고 수집시 목적과 추가처리 사이의 실질적 관계에 초점을 두고 분석해야 한다.[30] 또한, 개인정보처리자는 양립성을 분석·평가할 때 실제 상황과 함께 다양한 환경하에서 관련 이해당사자들이 처리 목적을 "공통적으로" 이해하는 방식을 항상 고려해야 한다.[31] 일반적으로 추가처리가 수집시의 목적과 현저히 다르거나 예측할 수 없는 것이라면 양립성은 인정되지 않는다. 이런 경우에는 정보주체의 명시적인 동의를 받아야 한다.[32]

유럽연합 WP29(2013)[33]는 1) 은행 계좌 개설 및 대출 계약시 수집한 신용정보를 1년 후 고객에게 더 유리한 대체 대출 및 저축 상품 안내 목적으로 이용한 경우, 2) 공무원 채용시 비밀취급인가 목적으로 실시한 신원조사결과를 추후 비밀취급업무 감사 목적으로 이용한 경우, 3) 공무원 채용시 정부지침에 따라 실시한 건강검진결과를 다른 정부부처와

30) Monica Iancu & Vasile Soltan, 앞의 글, p.3
31) 29WP, 앞의 의견서, pp.24-25
32) ICO, What is a 'compatible' purpose?
33) EU GDPR 제68조에서 규정하고 있는 유럽개인정보보호이사회(EDPB, European Data Protection Board)의 전신. WP29는 1995년 Directive 하에서 동 지침의 통일적인 적용을 위하여 설치된 작업반(Working Party)으로 지침의 해석, 권고, 조언, 의견서 작성 등의 역할을 수행하였으나 WP29의 행위는 법적 강제력을 인정받지 못했다. 이에 GDPR은 법적 지위와 권한을 부여받은 EDPB를 신설하고 WP29를 승계하도록 하였다.

공유한 경우, 4) 자동차등록사업소의 자동차 소유자 정보를 자동차제조회사의 리콜업무 이행 목적으로 제공한 경우, 5) 고객의 사기적인 에너지 이용 탐지를 위한 목적으로 스마트 미터링 정보를 분석 및 이용한 경우를 최초 수집 시의 목적과 관련성이 있는 것으로 보고 있다.

반면에, 1) 은행 계좌 개설 및 대출 계약시 수집한 고객정보를 보험상품 소개 목적으로 보험회사에 제공한 경우, 2) 직원채용 목적으로 수집한 인사정보를 자사제품 마케팅 활동에 이용한 경우, 3) 시장이 업무상 수집한 유권자 정보를 선거운동에 이용한 경우, 4) 보안 목적으로 회사 사옥 정문에 설치한 CCTV 영상정보를 근무에 소홀한 리셉션니스트의 근태감시 목적으로 이용한 경우, 5) 배차 승인 판단용 음주측정기를 근태(출근) 확인 목적으로 이용한 경우, 6) 슈퍼마켓이 고객의 개별 구매정보를 분석하여 정부가 추진하는 알코올 및 비만 예방 캠페인에 이용한 경우, 7) 여행 가이드가 촬영한 사진을 추후 새로 구축한 자사 웹사이트에 홍보 목적으로 이용한 경우, 8) 사진 공유 사이트에 업로드된 이용자의 사진정보를 회사가 자사 서비스 마케팅 목적으로 이용한 경우, 9) 비밀 알고리즘을 이용해 고객의 포인트카드 정보를 분석한 후 맞춤형 광고에 이용한 경우, 10) 개업의가 최근 퇴원한 환자목록을 요양 여행 소개 목적으로 여행사에 제공한 경우, 11) 지자체의 주택임차인 보조금 부서가 수집·구축한 임차주택DB를 화재예방 업무를 맡고 있는 주택부서와 공유한 경우, 12) 지자체의 교통체증 완화 정책수립 목적으로 통신사가 지자체에 고객의 휴대전화 위치정보를 제공한 경우, 15) 건강보조식품회사가 환자의 동의를 받아 병원 웹사이트에 포스팅해 놓은 개인정보를 수집해 자사 제품 마케팅 목적으로 이용한 경우 등은 수집 시의 목적과 관련성이 없는 것으로 보고 있다,

2. 개인정보가 수집된 정황(context). 특히 정보주체와 개인정보처리자의 관계

양립성을 평가할 때에는 개인정보가 수집된 정황 특히 개인정보처리자와 정보주체의 관계의 성격을 고려해야 한다. 개인정보처리자와 정보주체의 관계의 성격을 분석할 때에는 법률적인 요소뿐만 아니라 주어진 상황이나 주어진 관계에서 일반적으로 기대되는 관

행이 무엇인지도 고려해야 한다.[34] 특히 개인정보처리자와 정보주체 간의 힘의 균형을 조사해야 한다. 예컨대 정보주체가 해당 계약을 언제든지 쉽게 해지하고 다른 서비스로 이전할 수 있는지 여부를 검토해야 한다.[35]

개인정보처리자와 정보주체의 관계 등 수집시의 상황을 고려해서 정보주체가 추가처리를 합리적으로 예상할 수 있는 경우라면 양립성이 인정될 수 있다. 정보주체가 "합리적으로" 추가처리를 예상 또는 기대할 수 있었는지 여부는 정보주체와 같은 상황에 처해 있는 합리적인 제3자가 자신의 개인정보가 수집 시의 맥락에 비추어 추가처리를 예상할 수 있었는지 여부를 기준으로 판단해야 한다.

개인정보처리자와 정보주체의 관계의 성격에 비추어 보아 추가처리가 예상하기 어렵거나 놀라운 것이라면 양립성은 인정되지 않을 가능성이 높다. 일반적으로 힘의 불균형이 존재하는 관계(노사관계, 의사와 환자관계, 정보주체가 서비스를 선택할 수 있는 충분한 자유가 주어지지 아니한 경우)이거나 추가처리가 무례하거나 불쾌한 것으로 여겨질 수 있는 경우 양립성 평가는 더욱 엄격하게 실시되어야 한다. 반면, 개인정보처리자와 정보주체 간에 상품의 구매, 서비스 신청 등과 같은 거래관계가 있고 그 거래관계가 공평하다면 개인정보처리자가 정보주체로부터 수집한 이메일 주소로 마케팅 목적의 정보를 보내는 것 등은 합리적으로 예상할 수 있는 추가처리로 볼 수 있다.

유럽연합 WP29는 1) 은행 계좌 개설 및 대출 계약시 수집한 신용정보를 1년 후 고객에게 더 유리한 대체 대출 및 저축 상품 안내 목적으로 이용한 경우, 2) 비밀취급인가 목적으로 실시한 신원조사결과를 추후 비밀취급업무 감사 목적으로 이용한 경우, 3) 공개 알고리즘을 이용하여 고객의 포인트카드 정보를 분석한 후 맞춤형 광고(잔디깍기 판매)에 이용한 경우, 4) 자동차등록사업소의 자동차 소유자 정보를 자동차제조회사의 리콜업무 이행 목적으로 제공한 경우, 5) 고객의 사기적인 에너지 이용 탐지를 위한 목적으로 스마트 미터링 정보를 분석 및 이용한 경우에는 수집시의 정황을 고려할 때 정보주체가 합리적으로

34) Monica Iancu & Vasile Soltan, 앞의 글, p.3
35) 29WP, 앞의 의견서, pp.23-24

추가처리를 기대하거나 예상할 수 있었다고 판단하였다.

반면에, 1) 직원채용 목적으로 수집한 인사정보를 자사제품 마케팅 활동에 이용한 경우, 2) 보안 목적으로 회사 사옥 정문에 설치한 CCTV 영상정보를 근무에 소홀한 리셉션니스트의 근태감시 목적으로 이용한 경우, 3) 배차 승인 판단용 음주측정기를 근태(출근) 확인 목적으로 이용한 경우, 4) 사진 공유 사이트에 업로드된 이용자의 사진정보를 회사가 자사 서비스 마케팅 목적으로 이용한 경우, 5) 비밀 알고리즘을 이용해 고객의 포인트카드 정보를 분석한 후 맞춤형 광고에 이용한 경우, 6) 개업의가 최근 퇴원 환자 목록을 요양여행 소개 목적으로 여행사에 제공한 경우, 7) 지자체의 주택임차인 보조금 부서가 수집. 구축한 임차주택DB를 화재예방 업무를 맡고 있는 주택 부서와 공유한 경우, 8) 지자체의 교통체증 완화 정책수립 목적으로 통신사가 지자체에 고객의 휴대전화 위치정보를 제공한 경우, 9) 건강보조식품회사가 개업의가 환자의 동의를 받아 병원 웹사이트에 포스팅해 놓은 개인정보를 수집해 마케팅 목적으로 이용한 경우 등은 개인정보 수집시의 정황을 고려할 때 정보주체가 합리적으로 그와 같은 추가처리를 기대하거나 예상할 수 없는 경우라고 판단하였다.

3. 추가처리의 대상이 되는 개인정보의 유형 또는 성격(nature)

개인정보처리자는 추가처리하고자 하는 개인정보의 유형과 성격을 검토해야 한다. 즉, 추가처리되는 개인정보에 민감정보 또는 범죄정보가 포함되어 있지 않은지 여부를 검토해야 한다. 또한, 바이오 정보, 유전자 정보, 위치정보, 통신정보 등이 포함되어 있지 않은지 여부를 확인해야 하며, 그 밖에 특별한 보호를 받아야 할 개인정보가 포함되어 있지 않은지 검토해야 한다. 여기서 주의해야 할 점은 고려해야 할 정보가 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보 등 국내법상의 민감정보에 한정되지 않는다는 것이다.

사진정보, 금융정보, 위치정보 등은 주어진 맥락에 따라 사생활 침해 가능성이 클 수 있으므로 민감한 정보로 분류될 수 있다. 또한, 원본정보 그 자체는 민감하지 않아도 분석

도구(알고리즘, 소프트웨어 등)를 이용해서 분석한 결과인 추론정보(프로파일)는 민감한 정보가 되는 경우도 있다. 예컨대, 슈퍼마켓의 구매내역 정보는 민감하지 않지만 이를 분석하면 임신, 비만, 알콜중독 등의 여부를 알 수 있게 된다. 따라서 이 경우 분석결과(추론정보)는 민감성 정보로 취급해야 하다. 일반적으로 해당 개인정보가 민감한 정보일 수록 양립성을 인정할 수 있는 범위가 좁아진다.[36]

유럽연합 WP29(2013)는 슈퍼마켓의 구매이력, 은행의 계좌 개설 정보, 학부모의 연락처 정보, 백화점의 고객 구매정보, 소매체인의 구매이력 정보, 자동차 소유자의 자동차등록정보(이름, 연락처, 차종), 인터넷에 공개된 정보 등은 그 자체로만 이용된다면 민감한 정보로 보지 아니한다.

그러나 슈퍼마켓, 백화점, 포인트카드 등의 구매정보도 사생활 침해 가능성이 있는 결과를 도출할 목적으로 분석한 경우에는 민감한 정보로 보고 있으며(임신, 비만, 알콜중독 등의 결과 분석), 개인영상정보(CCTV영상정보), 사진정보, 위치정보, 통신정보, 스마트미터링정보, 환자목록, 음주측정정보, 책/영화/만화 등의 대출 및 구매 정보 등은 그 자체만으로도 민감한 정보로 본다. 또한, 음주측정기의 측정시간도 근태감시 목적으로 이용될 때는 민감한 정보로 보며, 인터넷에 공개된 정보(사진, 질병 등)도 공개 목적 외로 이용될 때는 민감한 정보로 보고 있다. 따라서 이와 같은 민감한 정보는 정보주체의 동의를 받거나 추가적인 보호수단이 강구되지 않으면 추가 목적으로 처리될 수 없다.

4. 추가처리가 정보주체에게 미치는 결과(possible consequence)

개인정보처리자는 추가처리가 정보주체에게 미칠 결과 또는 영향을 검토해야 한다. 추가처리의 영향을 평가할 때는 추가처리의 긍정적 결과와 부정적 결과를 모두 고려하여야 한다. 또한, 여기에는 제3자가 장래에 정보주체에게 취할 수 있는 잠재적인 결정 또는 행위, 추가처리가 정보주체의 배제 또는 차별로 이어질 수 있는 상황 등을 포함해야 한다. 구체적으로 예측이 가능한 불리한 결과(거래거절, 해고, 징계, 기소, 불합리한 차별대우

36) 29WP, 앞의 글, p.25 ; Monica Iancu & Vasile Soltan, 앞의 글, p.3

등) 외에도 정보주체가 느끼게 될 짜증, 공포, 고통, 압박감, 소외감, 수치심 등과 같은 정신적 영향도 고려해야 한다.[37]

추가처리가 정보주체에 미치는 영향을 분석할 때에는 추가처리의 방법도 포함해야 한다. 즉, 수집 시의 경우와 "다른" 상황에서 "다른" 개인정보처리자에 의해서 개인정보가 처리됨으로써 정보주체가 처리결과를 알 수 없는 상태인지 여부(제3자 제공), 개인정보가 일반에게 공개되거나 다수의 사람들에게 접근이 허용되는지 여부(개인정보의 공개), 대량의 개인정보가 다른 정보와 함께 처리되거나 결합되는지 여부(예컨대, 상업적 목적 또는 법집행 목적의 프로파일링), 특히 이와 같은 활동들이 수집 시에 예상할 수 있는 것이었는지 여부 등을 검토해야 한다.[38] 정보주체에게 미치는 영향(결과)은 다양한 크기와 범위로 존재할 수 있고, 구체화되고 제한적인 영향에서부터 일반적이고 예측할 수 없는 영향에 이르기까지 매우 다양할 수 있다.

개인정보처리자가 추구하는 목적을 달성할 수 있으면서도 정보주체에게 미치는 부정적 영향을 최소화 할 수 있는 대안적 방법이 있다면 그와 같은 사정도 양립성 평가시 반드시 고려해야 한다. 추가처리의 영향이 부정적이거나 불확실할수록 양립성은 인정되기 어렵다. 추가처리가 정보주체 또는 자연인에게 부당한 영향을 미친다면 양립성은 인정되지 않는다. 이런 경우에는 정보주체로부터 명시적인 동의를 받아야 한다.[39]

유럽연합 WP29(2013)는 1) 은행 계좌 개설 및 대출 계약시 수집한 신용정보를 1년 후 고객에게 더 유리한 대체 대출 및 저축 상품 안내 목적으로 이용한 경우, 2) 공개 알고리즘을 이용하여 고객의 포인트카드 정보를 분석한 후 맞춤형 광고(잔디깍기 판매) 목적으로 이용한 경우에는 정보주체에게 미칠 수 있는 잠재적인 영향의 결과가 정보주체에 불이익하지 않거나 오히려 유리하다고 평가하였다.

반면, 1) 은행 계좌 개설 및 대출 계약시 수집한 고객정보를 보험상품 소개 목적으로 보험회사에 제공한 경우, 2) 직원채용 목적으로 수집한 인사정보를 자사제품 마케팅 활동

37) Monica Iancu & Vasile Soltan, 앞의 글, p.3
38) 29WP, 앞의 의견서, pp.26-27
39) ICO, What is a 'compatible' purpose?

에 이용한 경우, 3) 보안 목적으로 회사 사옥 정문에 설치한 CCTV 영상정보를 근무에 소홀한 리셉션니스트의 근태감시 목적으로 이용한 경우, 5) 배차 승인 판단용 음주측정기를 근태(출근) 확인 목적으로 이용한 경우, 7) 여행 가이드가 촬영한 사진을 추후 새로 구축한 자사 웹사이트에 홍보 목적으로 이용한 경우, 8) 사진 공유 사이트에 업로드된 이용자의 사진정보를 회사가 자사의 서비스 마케팅 목적으로 이용한 경우, 9) 비밀 알고리즘을 이용하여 고객의 포인트카드 정보를 분석한 후 맞춤형 광고(임신부용 판매광고) 목적으로 이용한 경우, 10) 개업의가 최근 퇴원 환자 목록을 요양 여행 소개 목적으로 여행사에 제공한 경우, 11) 공무원 채용시 정부지침에 따라 실시한 건강검진결과를 다른 정부부처와 공유한 경우, 12) 지자체의 주택임차인 보조금 부서가 수집·구축한 임차주택DB를 화재예방 업무를 맡고 있는 주택 부서와 공유한 경우, 13) 지자체의 교통체증 완화 정책수립 목적으로 통신사가 지자체에 고객의 휴대전화 위치정보를 제공한 경우, 14) 건강보조식품회사가 환자의 동의를 받아 병원 웹사이트에 포스팅해 놓은 개인정보를 수집해 마케팅 목적으로 이용한 경우에는 정보주체에게 잠재적으로 불이익(경제적 불이익뿐만 아니라 해고, 징계, 차별, 소외, 압박감, 불쾌감, 짜증, 정보유출, 목적외 이용 등)을 줄 수 있다고 판단하였다.

한편, 1) 슈퍼마켓이 고객의 개별 구매정보를 분석하여 정부가 추진하는 알코올 및 비만 예방 캠페인에 이용한 경우, 2) 학교가 안전한 인터넷 교육을 받게 할 목적으로 비영리 교육단체에 학생과 학부모의 연락처정보를 제공한 경우, 3) 자동차등록사업소가 자동차제조회사의 리콜 의무 이행을 지원하기 위하여 자동차제조회사에 소유자의 이름, 연락처 등의 정보를 제공한 경우에는 잠재적으로 긍정적인 이익과 부정적인 이익이 공존한다고 보았다. 1)의 경우 알코올 및 비만 예방을 위한 맞춤형 건강정보를 제공받을 수 있는 장점이 있으나 알코올 중독 또는 비만이라는 부정적 이미지가 각인될 수 있다. 이 경우에는 정보주체의 동의를 받거나 계산대 앞에 건강정보를 비치하는 등의 대안적 방법을 모색해야 한다. 2)의 경우 인터넷의 안전한 이용방법에 관한 무료 교육이라는 이점에도 불구하고 개인정보가 제3자에게 제공됨으로써 목적외 이용, 정보유출 등의 위험이 존재한다. 이 경우에

도 학교는 정보주체의 동의를 받거나 개인정보를 제공하는 대신 학생과 학부모에게 해당 비영리 교육단체의 무료 교육 프로그램을 안내하는 등의 대안적 방법을 강구해야 한다. 3)의 경우 결함 자동차의 수리, 정보주체의 생명.신체 안전 등과 같은 긍정적 이익에도 불구하고 개인정보의 목적외 이용 가능성, 정보유출 위험 등이 공존한다. 이 경우 양립성을 인정받기 위해서는 개인정보의 목적외 이용 가능성, 유출 위험 등을 방지하기 위한 추가적인 보호조치(목적외 이용금지 계약의 체결, 암호화·침투테스트 등의 기술적·관리적 조치 등)가 강구되어야 한다.

5. 암호화, 가명화 등 적절한 보호수단의 존재(appropriate safeguards)

개인정보처리자는 양립성 평가시 개인정보의 공정한 처리를 보장하고 정보주체에 대한 과도한 영향을 방지하기 위하여 적용이 가능한 적절한 보호조치 또는 보호수단을 고려해야 한다. 보호조치 또는 보호수단은 앞에서 언급한 평가기준 또는 고려요소들을 통해서 드러난 양립성 평가의 부정적 결과를 보완해 줄 수 있는 기회를 개인정보처리자에게 제공해주기 위한 것이다.[40] 수집 시의 처리 목적과 추가처리의 거리가 멀면 멀수록 보호조치 또는 보호수단은 보다 효과적이고 신중해야 한다. 다시 말해 보호조치는 목적 간의 거리에 비례해야 한다. 또한, 추가처리와 관련하여 제공되는 여러 보증 수단들은 최소한 최초 처리 시에 제공되는 것과 동일한 수준을 계속 유지해야 한다.

양립성 평가의 부정적 결과를 보완해 줄 수 있는 보호조치 또는 보호수단의 예로는 익명화, 가명화, 총계화, 그 밖의 개인정보보호기술(PETs) 등과 같은 기술적 수단이 있을 수 있고, 정보주체에 대한 추가적인 정보의 제공, 양립성 평가 방법 및 결과의 공개를 통한 투명성 제고, 정보주체에게 양립성 평가를 거부할 수 있는 기회의 제공, AI 분석 도구의 알고리즘 원리 설명 등과 같은 비기술적 방법도 있다.[41][42] 예컨대, 공무원 채용시 정

40) ICO, What is a 'compatible' purpose?
41) 29WP, 앞의 의견서, pp.25-26
42) Monica Iancu & Vasile Soltan, 앞의 글, p.4

부지침에 따라 실시한 건강검진결과를 비용절감, 시간절약 등을 위해 정부부처 간에 공유하기로 합의한 경우 불합격한 건강검진 결과는 공유대상에서 삭제하여 지원자가 다른 정부부처의 채용절차에 지원할 수 있는 기회를 보장하는 것도 보호조치의 하나이다. 또한, 지자체가 교통체증 완화 정책 수립을 위해 통신사에게 고객의 휴대전화 위치정보를 요구할 때에는 제공하기 전에 엄격한 익명화, 모의 침투 테스트, 주의 깊은 영향평가, 이해당사자 자문, 제공 목적의 투명한 공개 등과 같은 추가적인 보호조치 또는 보호수단을 강구해야 한다.

이상과 같은 추가적인 보호조치를 통해서도 나머지 고려요소의 결점 또는 결함을 보완할 수 없다면 추가처리에 대해서 정보주체의 동의를 받아야 한다.

Ⅵ. 양립성 평가의 사례 분석

우리나라에서는 양립성 규정의 도입을 계기로 고객 또는 이용자의 개인정보나 행태정보를 분석하여 맞춤형 광고가 가능할지에 대해서 관심이 크다. 따라서 본장에서는 WP29(2013)가 맞춤형 광고 목적의 추가처리에 대하여 극명하게 대비되는 판단을 내린 두 개의 양립성 평가 사례의 분석을 통해서 양립성 평가를 통해서 맞춤형 광고가 가능한지 여부, 가능하다면 어디까지 가능한지 여부 등에 대해서 살펴보고자 한다. 이를 통해 양립성 평가의 본질을 더욱 잘 이해할 수 있게 될 것이다.

[사례1] 고객의 포인트카드 정보를 맞춤형 광고(임신부 용품 판매) 목적으로 비밀 알고리즘을 이용하여 분석[43)]

(시나리오) A백화점은 고객의 구매습관을 분석하고, 새로운 마케팅 트렌드를 파악하고, 고객에게 특별한 제안을 하고, 할인쿠폰을 보내기 위해 고객의 포인트카드 정보를 이용하

43) 29WP, 앞의 의견서, p.61

고 한다. 백화점이 이용하고 있는 분석 소프트웨어는 여성 고객의 임신 여부는 물론 임신 개월 수까지 비교적 정확히 분석이 가능하다. 고객의 포인트카드 정보는 고객의 프로파일에 맞추어 맞춤형 마케팅을 제안하기 위해 이용된다. 고객이 포인트 카드를 등록(가입)할 때에는 개인정보 이용에 관하여 고객에게 어떤 정보도 제공되지 않는다. 다만, 백화점 웹사이트에 게시되어 있는 약관에는 '포인트 카드 정보는 고객에 대한 특별 제안 및 할인쿠폰 제공을 포함해 마케팅 목적으로 이용된다.'고 기술되어 있다. 이에 근거하여 백화점은 고객의 주소로 임신부 용품의 판매 촉진을 위한 맞춤형 전단을 보냈다. 고객의 아빠는 가족의 메일 박스에 임신부 관련 광고물이 쌓인 것을 의아하게 생각하다가 자신의 10대 소녀인 딸이 임신 3개월째라는 사실을 알게 된다.

(평가결과) 결론부터 말하면 이 사례는 의심의 여지없이 프라이버시 문제를 야기하므로 양립성이 인정되지 않는다. 첫째, 소녀가 포인트카드에 가입한 목적과 맞춤형 광고 사이에는 관련성이 없다. WP29는 목적 관련성에 대해서는 명시적으로 언급하고 있지 않다. 그러나 관련성 유무를 고려할 때에는 이해당사자들이 처리 목적을 "공통적으로" 이해하는 방식으로 평가해야 하는 바 포인트카드 회원 가입시 어느 정도의 마케팅은 예상할 수 있다고 해도 프로파일링을 통한 맞춤형 광고까지 관련성이 있다고 보기는 어려울 것이다.

둘째, 백화점은 고객에게 알고리즘을 이용한 프로파일링 사실과 알고리즘의 분석 방법(임신 사실의 분석 방법)을 투명하게 공개하지 않았으며, 맞춤형 광고 서비스를 자유롭게 선택할 수 있는 기회도 제공하지 않았다. 이용 약관에 포인트카드 정보를 마케팅 목적으로 이용한다는 내용이 기술되어 있기는 하지만 고객에게 선택권이 주어져 있지 않으므로 불공평하고 불공정하다.

셋째, 포인트카드 정보 그 자체(구매일시, 구매상품, 구매가격 등)는 사생활 침해 가능성이 특별히 높다고 할 수 없지만, 수집된 개인정보를 결합해서, 추가처리하고, 비밀 알고리즘을 이용해서 분석할 결과인 프로파일(임신 여부, 임신 개월 수 등의 추론정보)은 매우 민감한 정보에 해당한다.

넷째, 대다수 초기 임신부들은 임신 사실을 자기 자신 또는 소수의 가족 및 친구하고만 공유하고 싶어 한다. 또한, 대다수 일반 고객은 임신을 예측하기 위해서 비밀 알고리즘을 이용하여 프로파일링을 수행하는 것에 대해서 예상하기 어렵고, 부적절하며, 불쾌하다고 생각한다. 따라서 정보주체의 이익이 침해되었다.

마지막으로, 백화점은 정보주체의 권리보호를 위한 적절한 보호조치를 취하지 않았다. 백화점은 전혀 기대하거나 예상하기 어려운 불가사의한 임신 예상 알고리즘을 이용하여 고객에게 맞춤형 마케팅을 시도하였다. 구매이력 정보는 외견상 전혀 위험하지 않은 정보이므로 누구도 그와 같은 방식의 프로파일링을 예상하기 어렵다. 대중의 합리적인 기대에 부합하지 않은 방식 또는 대중에게 불공정하고 불유쾌한 방식으로 설계된 알고리즘은 정보주체의 자유롭고 명시적인 동의에 의해서만 가능하다.

[사례2] 고객의 포인트카드 정보를 맞춤형 광고(전용원 잔디깍기 판매) 목적으로 공개 알고리즘을 이용하여 분석[44)]

(시나리오) B원예용품판매점은 전국적으로 소매체인을 두고 잔디깍기 등 원예용품을 판매하고 있다. 원예용품판매점은 고객이 포인트카드를 이용해 상품을 구입할 경우 모든 상품에 대해서 10%의 할인을 제공한다. 회사 웹사이트에는 개인정보처리방침이 공개되어 있으며, 포인트카드 가입 고객에 대해서는 요약 버전의 개인정보처리방침이 별도로 제공된다. 회원 가입시 고객에게는 명확하게 문서로 작성된 두 가지 옵션이 제공되는데 고객은 그중 하나를 자유롭게 선택할 수 있다. 옵션1은 '나의 구매 이력을 온라인에 저장하고 이를 이용해 나의 구매 행태를 분석한 후 나에게 맞는 맞춤형 할인 및 맞춤형 제안을 제공받기'이고, 옵션2는 '나의 개인정보를 비공개로 하고 일반적인 할인(10% 할인)만 제공받기'이다. 보다 상세한 설명이 온라인과 오프라인을 통해서 제공된다. 또한, 포인트카드 고객은 온라인을 통해서 자신에게 제공된 맞춤형 추천 상품의 내용뿐만 아니라 회사가 미리 설정해 놓은 방식으로 자신의 지난 5년간의 구매이력도 조회할 수 있다. 고객은 표준화된

44) 29WP, 앞의 의견서, pp.61-63

포맷으로 자신의 구매이력을 다운로드 받아 저장해 두었다가 자신의 재무상태를 분석하는데 이용할 수도 있다.

그 밖에 웹사이트는 고객의 구매이력을 분석해 고객이 좋아할 만한 상품을 추천할 수 있는 이용자 친화적인 기능을 다수 포함하고 있으며, 데이터 분석 소프트웨어가 어떻게 작동하는지 분석 방법에 대해서도 공개하고 있다. 예컨대, 고객에 대한 할인 제안은 고객이 이전에 구매한 품목에 대해서 교체를 생각할 무렵에 전송되는데 교체 시기는 주로 제품의 생명주기 등 업계의 실태와 관행을 고려한다고 안내하고 있다. 또한, 고객에게 제공되는 할인율은 고객이 매월 구매하는 평균 이용액(이용액이 많은 수록 높은 할인율을 적용), 할인 제안의 이용 경험 및 정도(이전에 제시한 할인상품을 구매했는지 여부), 그밖에 투명하고 자세하게 설명된 관련 지표 등을 기반으로 해서 고객별로 맞춤화하게 된다고 안내하고 있다. 옵션1의 "맞춤형 할인"을 선택한 정원사는 최근 자신의 잔디깍기 기계가 몇 차례 고장을 일으키기 시작할 무렵 원예용품판매점으로부터 새 브랜드로 잔디깍기 기계를 교체하면 30%의 할인을 제공하겠다는 제안을 받았다.

(평가결과) 본 사례에서 회원에 대한 맞춤형 서비스 제안을 목적으로 한 포인트카드 회원정보의 이용은 추가처리가 가능하다. 첫째, 포인트카드 회원 가입시 고객에게 명확하게 문서로 작성된 옵션을 제공하였고 고객이 자유롭게 선택한 옵션에 따라 맞춤형 마케팅 서비스를 전송한 것이므로 회원가입 목적과 맞춤형 할인 사이에 관련성이 존재한다. 다만, WP29는 목적 관련성에 대해서는 명시적으로 언급하고 있지 않다.

둘째, 원예용품판매점은 옵션의 내용을 투명하게 공개하고 고객에게 자유롭게 선택할 수 있는 기회를 제공하였으므로 불공평하거나 불쾌하지 않다. 고객이 맞춤형 마케팅 서비스를 원하지 아니할 경우 옵션2를 선택하면 되고, 이 경우 고객에 대한 프로파일링 없이 모든 회원에게 획일적으로 제공되는 일반적인 할인(10%) 혜택을 받을 수 있으므로 공평하고 공정하다.

셋째, 데이터의 성격이 민감하지 않다. 정원용품의 구매 이력정보도 상세히 분석하면

정보주체에게 침해적인 영향을 미칠 수 있으나, 웹사이트 방문 이력, 책 또는 영화의 구매·대여 이력, 의약품의 구매 이력 등으로부터 추론된 정보만큼 침해적이지 않다. 따라서 이와 같은 알고리즘의 작동 방식(제품의 수명주기를 계산한 제안 결정 방식), 분석대상 개인정보의 성격, 분석결과의 낮은 침해성이라면 민감한 성격의 정보라고 할 수 없다.

넷째, 예측가능하고 합리적인 방식으로 고객을 프로파일링하도록 알고리즘이 설계되어 있고, 알고리즘의 작동원리가 투명하게 공개되어 있으며, 고객이 제품을 교체해야 할 시기에 적기에 새로운 제품을 제안함으로써 고객을 불편하게 하기보다는 오히려 고객에게 편의를 가져다 준다. 특히 제품의 일반적인 수명주기를 계산해서 제안하므로 사생활 침해가 없고 놀랍거나 불쾌한 방식도 아니다.

마지막으로, 원예용품판매점은 마케팅 목적의 추적과 프로파일링에 대해서 고객에게 충분한 정보를 제공하고 자유롭게 선택할 수 있는 기회를 제공하기 위해 많은 노력을 기우리고 있다. 이는 정보주체에게 공정할 뿐만 아니라 예상치 못하거나 불쾌한 영향을 최소화한 것이다. 또한 스스로 프로파일링을 위한 알고리즘(맞춤형 광고의 결정기준)을 투명하게 공개함으로써 불공정하거나 불쾌한 방식으로 개인정보를 사용할 가능성을 줄이는 등 정보주체의 이익을 보호하기 위한 적절한 보호조치를 강구하였다.

이상 두 사례의 차이를 정리하면, 전자는 프로파일링의 방법을 비공개로 하고 있고, 알고리즘의 설계가 사생활 침해적인 방식이며, 정보주체에게 선택할 기회를 제공하고 있지 않은 반면, 후자는 프로파일링의 방법을 투명하게 공개하고 있고, 알고리즘의 설계방식이 예측가능하고 합리적이며, 정보주체에게 충분히 선택할 수 있는 기회를 주고 있다는 점이다.

Ⅶ. 양립성 평가의 면제와 배제

1. 양립성 평가의 면제 : 양립성의 간주

가. 역사적, 과학적 및 통계적 목적의 추가처리

공공의 이익을 위한 기록보관 목적, 과학적 또는 역사적 연구 목적, 통계적 목적을 위한 추가처리는 GDPR 제89조제1항[45]에 따라 가명화, 익명화 등을 포함하여 정보주체의 권리와 자유를 보호하기 위한 적절한 보호조치 특히 개인정보 최소처리원칙을 보장하기 위한 기술적·관리적 조치가 취해졌다면 법률에 의하여 당초의 수집 목적과 양립할 수 있는 것으로 간주된다(제5조제1항(b)). 따라서 공익적 기록, 역사적, 과학적 및 통계적 목적의 개인정보 추가처리는 제6조제4항에 따른 양립성 평가를 할 필요는 없다.[46]

다만, 이 경우에도 모든 유형의 공익적 기록, 역사적, 과학적 및 통계적 목적의 추가처리에 대해서 당연히 양립성이 간주되는 것은 아니다. 공익적 기록, 역사적, 과학적 및 통계적 목적의 추가처리에 대하여 양립성 평가를 면제받기 위해서는 적절한 보호조치(appropriate safeguards)를 통해서 목적 변경에 따른 개인정보 침해 위험을 상쇄시켜야 하고, 이를 통해서 특정 개인에 대한 어떤 조치를 내리거나 의사결정을 내리는데 이용

45) Art. 89 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

46) WP29는 1995년 Directive 제6조제1항(b)(현행 GDPR 제5조제1항 (B))의 문구만으로는 과학적 연구 등 목적의 처리에 대해 양립성 평가가 면제되는지 여부가 불분명하다고 하면서도 양립성 평가규정에 대한 특별규정으로서의 성격을 인정하고 있다(WP29, p.13, p39). 다만, 적절한 안전조치를 취하고 있어야 양립성 평가가 면제될 수 있다(WP29, p.28).

되지 못하도록 보장을 해야 한다.[47] 즉, 개인정보가 특정 개인에 대한 어떤 조치를 내리거나 의사결정을 내리는데 이용되지 못하도록 보장해야 한다. 이를 통해 정보주체에 대한 부정적 영향은 물론 긍정적 영향도 피해야 한다.

공익적 기록, 역사적, 과학적 및 통계적 목적을 위한 적절한 보호조치의 수준과 방법은 연구의 특성에 따라 i) 합리적으로 더 이상 정보주체를 식별할 수 있는 가능성을 남기지 않는 방법으로 개인정보를 익명화하거나 총계화하거나, ii) 하위 수준의 총계화, 부분적인 익명화(pseudo-anonymisation, key-coding, keyed-hashing, using rotating salts, removal of direct identifiers 및 outliers, replacing unique IDs, introduction of noise 등), 가명화, 키코드화(key-coding) 등을 통해 간접적으로만 식별이 가능하게 하거나, iii) 불가피한 경우에는 직접 식별이 가능한 상태로 처리하되 다른 추가적인 안전조치(암호화, 분리보관 등)를 취할 수 있다.[48]

또한, 공익적 기록, 역사적, 과학적 및 통계적 목적을 위한 추가처리라 하더라도 건강정보, 아동정보, 취약계층의 개인정보, 그 밖에 매우 민감한 정보는 원칙적으로 정보주체의 동의를 받아야 한다. 이런 유형의 개인정보 추가처리에 대한 동의의 면제는 정보주체에 대한 과도한 영향을 방지하기 위한 기술적·관리적 조치를 포함하여 적절한 보호조치의 강구와 함께, 법률에 명시적인 근거가 있거나 중대한 공공의 이익을 위한 연구로써 그 연구가 달리 수행될 수 없는 경우에만 허용된다.[49]

나. 광고성 정보 전송 목적의 추가처리

유럽연합에서는 자동전화시스템, 팩스, 이메일 등을 이용해서 다이렉트 마케팅(직접판매) 목적으로 광고성 정보를 전송하기 위해서는 사전에 이용자로부터 광고성 정보 수신에 대한 명시적인 동의(opt-in)를 받아야 한다. 그러나 사업자가 이전에 소비자에게 물품 또는 서비스를 제공하면서 소비자로부터 직접 수집한 이메일 주소를 이용하여 이전에 판매

47) 29WP, 앞의 의견서, p.28
48) 29WP, 앞의 의견서, pp.28-33
49) 29WP, 앞의 의견서, pp.32-33

한 것과 유사한 물품 또는 서비스를 홍보하기 위한 광고성 정보를 전송할 때에는 동의를 요하지 않는다. 사업자와 소비자 사이에 거래관계가 존재하고 소비자가 직접 제공한 이메일 주소를 이용하여 소비자가 구매한 것과 유사한 물품 또는 서비스에 관한 광고성 정보만을 전송하므로 소비자가 합리적으로 추가처리를 기대할 수 있는 상황이라고 본 것이다.[50] 따라서 이와 같은 광고성 정보 전송 목적의 추가처리에 대해서는 양립성 평가가 필요하지 않다.

그러나 일반우편과 같은 전통적 수단을 이용해서 상업적, 정치적 및 자선적 목적의 개인화된 메시지를 전송하는 경우에는 동의가 면제되지 않으므로 양립성 평가에 의해서도 다이렉트 메일을 보낼 수 없다. 또한, 정보주체와의 사이에 기존의 거래관계가 있기는 하지만 다른 물품 또는 서비스에 관한 정보를 제공하기 위하여 다이렉트 메일을 보내는 경우, 다이렉트 메일이지만 민감한 개인정보를 이용하거나 보다 침해적인 데이터 분석 수단을 이용해(즉, 자동화된 프로파일링을 이용해) 다이렉트 메일을 보내는 경우, 다이렉트 메일링을 보다 효과적으로 세분화하기 위해 데이터 판매상 또는 다른 제3자와 정보를 공유하는 경우 등에도 동의를 받아야 한다.[51]

우리나라의 경우 「정보통신망 이용촉진 및 정보보호등에 관한 법률」(이하 “정보통신망법”이라 한다)에 따라 재화등의 거래관계를 통해 수신자로부터 직접 연락처를 수집한 자가 해당 재화등의 거래가 종료된 날부터 6개월 이내에 수신자와 거래한 것과 동종의 재화등에 대한 영리목적의 광고성 정보(스팸)를 전송하는 경우에는 수신자의 동의를 받을 필요가 없다(제50조제1항 단서). 그럼에도 불구하고 광고성 정보 전송 목적의 개인정보 이용에 대해서는 동의 의무가 면제되지 않는다는 이유로 동의가 요구되어 왔다. 양립성 규정의 신설로 이제 국내에서도 정보통신망법 제50조제1항 단서에 해당하는 경우에는 양립성이 인정되어 동의를 받을 필요가 없다는 해석이 가능할 것으로 보인다.

50) 29WP, 앞의 의견서, pp.34-35
51) 29WP, 앞의 의견서, pp.34-35

2. 양립성 평가의 배제 : 양립성의 불인정

가. 빅 데이터의 추가처리

GDPR에서는 적절한 수준의 보호조치 의무만 이행한다면 공익적 기록, 역사적, 과학적, 통계적 목적을 위한 개인정보의 추가처리에 대해서는 정보주체의 동의를 받을 필요가 없고 양립성 평가를 수행할 필요도 없다. 그러나 기업, 정부, 그 밖의 크고 작은 조직들이 컴퓨터 알고리즘을 이용하여 광범위하게 분석하는 거대한 디지털 데이터 셋인 빅 데이터의 경우는 다르다. 자동화 기술을 이용하여 정보의 가용성과 분석력을 획기적으로 증대시킨 빅 데이터는 일반적인 트렌드(general trends) 분석이나 상관관계(correlations) 식별을 위해서 사용되기도 하지만, 개인에 대한 "조치 또는 결정(measures or decisions)"을 통해 직접적인 영향을 미칠 목적으로 처리될 수도 있기 때문이다.

빅데이터의 궁극적인 목적은 보다 많은 정보를 통해서 보다 정확한 결정을 내리고자 하는 것이다. 때문에 헬쓰케어, 이동통신, 스마트그리드, 트래픽 관리, 사기행위 탐지, 마케팅, 소매 등 다양한 분야에서 빅 데이터 기술이 활용되고 있다. 예컨대, 마케팅 또는 광고 분야에서 빅 데이터를 이용하여 개별 고객의 취향, 행동, 태도 등을 분석 또는 예측하고, 이를 통해 고객의 프로파일을 기반으로 개인화된 할인 제공, 특별 제안, 타케팅 광고 등을 할 수 있다. 이 경우 빅 데이터는 출처를 알 수 없는 다양한 소스로부터 수집된 정보의 결합 및 처리, 개인 추적 및 프로파일링, 의도적이든 비의도적이든 불합리한 알고리즘에 의한 부정확한 판단, 불공정하거나 차별적인 결정, 경제적 불균형의 확대 및 배제 등의 부작용(가격차별, 고용기회, 대출이자, 보험료 등)을 낳을 수 있다.

이와 같은 부작용과 우려 때문에 WP29(2013)는 일반적인 트렌드 분석이나 상관관계 식별 목적의 빅 데이터 추가처리에 대해서는 엄격한 수준의 양립성 평가(충분한 익명화 또는 총계화)의 적용을 허용하고 있지만, 특정 개인에 대한 조치 또는 결정으로 이어질 수 있는 개인의 취향, 행동, 태도 등의 분석 또는 평가를 목적으로 하는 빅 데이터의 추가처리에 대해서는 양립성 평가를 적용할 수 없다는 입장이다. 이 경우에는 정보주체에게

동의에 필요한 충분한 정보를 제공한 후 자유롭고 구체적이며 명시적인 “동의(opt-in)”를 받아야 한다는 것이다. 예컨대, 직접 마케팅, 행태 광고, 데이터 브로커링, 위치기반 광고, 추적기반 디지털 시장조사 등을 위한 추적과 프로파일링에 대해서는 명시적인 동의를 받아야 한다.[52]

나. 오픈 데이터의 재사용

오픈 데이터는 공공기관이 보유하고 있는 대량의 개인정보 데이터베이스를 표준화된 전자적 형태로 일반인에게 공개하는 것으로, 공공기관이 보유하고 있는 정확하고 활용성 높은 개인정보에 대한 수요에 부응하고자 하는 것이다. 공공기관이 적법하게 공개한 정보라고 하더라도 식별이 되거나 식별이 가능한 개인에 관한 정보는 공개적으로 이용이 가능하든 이용할 수 없든 개인정보로 간주되며, 공개적으로 이용이 가능하다는 사실만으로 개인정보 보호법의 적용이 면제되지 않는다. 따라서 공공기관이 공개한 개인정보의 “재사용(reuse)”에 대해서도 개인정보 보호법을 준수해야 한다.

이에 따라, 공공기관이 오픈 데이터를 재사용하기 위하여 공개할 때에는 원칙적으로 익명화, 총계화 등의 비식별 조치의 절차를 거쳐야 한다. 오픈 데이터의 경우에도 주로 통계적 목적으로만 이용되는 경우와 개인별 데이터 분석이 필요하거나 개인 식별이 필요한 경우가 있을 수 있다. 후자의 경우에는 재사용의 성격과 목적 때문에 오픈 데이터를 익명화하기 어렵다. 오픈 데이터를 통계적 목적으로 이용한다면 충분히 익명화하거나 총계화해서 이용하면 되지만, 세밀한 분석이 필요한 연구(granular research)나 개인 식별이 필요한 연구에 대해서는 익명화 또는 총계화가 어렵기 때문에 원칙적으로 오픈 데이터의 재사용은 적절하지 않다는 것이 WP29의 입장이다.[53]

이 경우 익명화 또는 총계화는 오픈 데이터를 제공 또는 공개하기 전에 해야 하며, 공공

52) 29WP, 앞의 의견서, pp.45-47 ; Cédric Burton, European Regulators Opinion on “Purpose Limitation” Principle – What Constitutes “Compatible Use” in the Context of Big Data?, May 15, 2013, pp.2-3

53) 29WP, 앞의 의견서, pp.48-50

기관이 직접 수행하거나 신뢰할 수 있는 제3의 기관(TTP)을 통해서 수행해야 한다. 그러나 충분히 익명화를 했다고 해도 당시에는 재식별이 가능한지 여부를 평가하기 어려운 회색 지대가 많으므로 WP29는 익명화된 데이터 셋을 제공하거나 공개할 때에는 미리 개인정보 영향평가를 실시할 것을 권고하고 있다.[54] 빅 데이터와 달리 오픈 데이터는 공공기관이 국민의 사전 동의(opt-in)를 받는 것이 사실상 불가능하므로 동의에 의한 오픈 데이터 재사용은 어렵다.

Ⅷ. GDPR 양립성 규정이 국내법에 미치는 함의 및 시사점

1. 양립성 평가가 적용될 수 있는 추가처리의 범위

GDPR는 최초 수집 활동 이외의 모든 처리 활동을 추가처리로 보기 때문에 추가 "목적" 이외에 이용·제공되는 개인정보의 항목, 이용·제공 기간, 제공받는 자 등도 양립성 평가에 의해서 추가·확대할 수 있음이 명확하다. 그러나 개인정보 보호법은 당초 수집 "목적"과 합리적으로 관련된 범위에서 이용 및 제공할 수 있다고 규정하고 있어 추가처리의 대상이 명확하지 않다. 즉, 이용·제공의 "목적"만 양립성 평가의 대상인지 이용·제공 및 보관의 기간, 이용·제공하는 개인정보의 항목, 제공받는 자 등도 양립성 평가에 의해서 추가·확대가 가능하지 분명하지 않다. 양립성 제도의 취지를 고려할 때 개인정보의 처리기간, 처리항목, 제공받는 자에 대해서도 "합리적으로 관련된 범위 내"에서 연장 및 확대가 가능하다고 보아야 할 것이다. 다만, 양립성 평가에 의해서도 새로운 개인정보의 "수집"은 불가능하다고 보아야 한다.

54) 29WP, 앞의 의견서, pp.48-50

2. 양립성 평가에 의해 추가처리가 가능한 개인정보의 대상

GDPR은 양립성 평가에 의해서 추가처리를 할 수 있는 개인정보의 대상을 정보주체와 체결한 계약이행을 위하여 수집한 개인정보, 정보주체 또는 자연인의 중대한 이익보호를 위하여 수집한 개인정보, 개인정보처리자 또는 제3자의 정당한 이익 추구를 위하여 수집한 개인정보로 한정하고, 정보주체의 동의나 법률의 규정에 의하여 수집한 개인정보에 대해서는 양립성 평가에 의한 추가처리를 인정하지 않고 있다. 그러나 우리나라는 이와 같은 제한이 없다. 우리나라의 경우 동의의 예외 요건을 엄격히 해석하고 있고 특히 정보통신서비스제공자의 경우 동의를 원칙으로 하고 있어 동의에 의해서 수집된 개인정보에 대해서 양립성 평가를 통한 추가처리를 허용하지 않을 경우 양립성 규정의 효용이 반감할 것으로 예상된다.

〈표 1〉 양립성 요건에 따라 추가처리가 가능한 개인정보 비교

적법처리 근거	EU GDPR	개인정보 보호법
1. 정보주체의 동의를 받은 경우	불인정	인 정
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우	불인정	인 정
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우	불인정	인 정
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우	인 정	인 정
5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우	인 정	인 정
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우	인 정	인 정

3. 개인정보 수집시의 정황 및 관행의 고려

GDPR은 양립성을 평가할 때 개인정보가 수집된 정황 특히 정보주체와 개인정보처리자 간의 관계를 고려하도록 요구하고 있다. 이 경우 개인정보처리자와 정보주체의 관계를 분석할 때는 특히 양자 사이의 “힘의 불균형” 유무를 살펴야 한다. 예컨대 사용자와 근로자의 관계, 의사와 환자의 관계, 서비스의 선택 가능성, 서비스 이전의 곤란성, 정보주체

의 취약한 입장(곤궁한 입장) 등을 고려해야 한다. 노사관계와 같이 힘의 불균형이 명백한 경우뿐만 아니라, 서비스의 선택 가능성과 서비스 이전 용이성도 고려의 대상이라는 점이 특징이라고 할 수 있다. 또한, 정보주체로부터 직접 수집하지 않고 제3자나 공개된 장소로부터 간접적으로 수집한 정보에 대해서도 보다 엄격한 양립성 평가가 요구된다. 힘의 불균형이 존재하는 경우에는 추가처리에 대한 정보주체의 예측 가능성을 보다 엄격하게 판단하게 된다.

4. 기대 가능성 또는 예측 가능성의 판단주체

추가처리에 대한 정보주체의 기대 가능성 또는 예측 가능성을 고려할 때에는 개인정보가 "수집된 정황"을 고려해서 판단해야 한다. 수집시의 정황에는 개인정보처리자와 정보주체 간의 관계의 성격뿐만 아니라 주어진 상황에서 개인정보의 "처리 관행"도 포함된다. 수집된 정황을 고려해서 기대 가능성을 판단해야 한다는 것은 정보주체와 같은 상황에 처해 있는 "합리적인 제3자"의 시각에서 평가되어야 함을 의미한다. 정보주체가 처한 특이한 조건(교육 수준, 사회 경험, 지적 능력 등)은 특별한 사유가 없는 한 고려대상이 되지 못한다. 그러나 추가처리가 가져올 사회·경제적 효과는 정보주체의 이익을 침해하지 않는 범위 내에서 고려의 대상이 될 수 있다고 본다.

5. 개인정보의 성격(특성)의 고려 여부 문제

GDPR에서는 민감정보, 범죄정보 등도 원칙적으로 추가처리의 대상에서 배제되지는 아니하나, 이와 같은 정보는 사생활 침해 가능성이 높기 때문에 양립성 평가를 통해서는 사실상 추가처리가 어렵다. 민감정보, 범죄정보 등뿐만 아니라 사진정보, 금융정보, 통신정보, 위치정보, 출퇴근정보, 음주측정결과 등도 맥락에 따라 민감한 정보로 분류될 수 있고, 원본정보 그 자체는 민감하지 않더라도 분석 도구(알고리즘, 소프트웨어 등)를 이용해서 분석한 결과인 추론정보는 민감한 정보로 분류되며, SNS나 인터넷에 적법하게 공개된

정보도 공개 목적과 달리 이용될 때에는 민감한 정보로 취급된다. 따라서 이와 같은 “민감성 정보”는 양립성 평가를 통한 추가처리가 제한된다.

이에 반해 우리나라 개인정보 보호법은 민감정보, 고유식별정보 및 개인영상정보는 양립성 평가대상에서 제외하고 있는 것으로 해석되나, 그밖의 “민감성 정보”는 양립성 평가대상에서 제외되어 있지도 않고 고려사항에 포함되어 있지도 않다. 즉, 우리나라 개인정보 보호법은 GDPR과 달리 “개인정보의 유형 또는 성격”을 양립성 평가시 고려대상에 명시하고 있지 않다. 국내법상 개인정보의 유형 또는 성격이 양립성 평가의 고려항목에서 빠져있기는 하지만 양립성 평가에서 개인정보의 성격이 차지하는 중요성을 고려할 때(특히 프로파일 정보) “정보주체에게 미치는 영향”을 평가할 때라도 반드시 개인정보의 성격 또는 특성을 고려해야 할 것이다.

〈표 2〉 GDPR과 국내법 간 양립성 평가요소 비교

GDPR(고려사항)	개인정보보호법(필수요건)	신용정보법(고려사항)
개인정보의 최초 수집시 목적과 의도된 추가처리 목적 간의 관련성	개인정보를 추가적으로 이용하려는 목적이 당초 수집 목적과 상당한 관련성이 있을 것	양 목적 간의 관련성
개인정보가 수집된 정황. 특히 정보주체와 개인정보처리자 간의 관계의 성격	개인정보를 수집한 정황과 처리 관행에 비추어 볼 때 추가적으로 이용할 수 있을 것으로 예측 가능할 것	신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경위
개인정보의 성격, 특히 특별범주 또는 범죄와 관련된 개인정보인지 여부	X (단, 민감정보, 고유식별정보, 개인영상정보는 제외)	X
정보주체에게 미칠 수 있는 추가처리의 가능한 영향(결과)	개인정보의 추가적 이용이 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니할 것	해당 개인신용정보의 제공이 신용정보주체에게 미치는 영향
암호화 또는 가명화를 포함하여 적절한 보호수단의 존재	가명처리를 하여도 추가적 이용 목적을 달성할 수 있는 경우에는 가명처리하여 이용할 것	가명처리를 하는 등 신용정보의 보안대책을 적절히 시행하였는지 여부

6. 정보주체에게 미칠 것으로 예상되는 영향의 유형

GDPR은 추가처리가 정보주체에게 미칠 수 있는 "가능한" 영향(결과)에 대해서 고려하도록 규정하고 있으므로 이와 같은 영향에는 부정적 영향(불이익)은 물론 긍정적 영향(이익)도 고려해야 하고, 현실적인 이익 또는 불이익뿐만 아니라 잠재적 이익 또는 불이익도 고려해야 한다. 이 경우 불이익은 경제적 불이익뿐만 아니라 기소, 징계, 해고, 차별 등과 같은 불이익도 포함되며, 성가심, 불안, 불편함, 짜증유발, 스트레스, 압박감, 따돌림, 소외감 등과 같은 정신적 고통도 고려의 대상이다. 이와 같은 불이익은 반드시 "부당한" 것이어야 한다는 요건도 없다. 예컨대 추가처리의 결과에 따라 정보주체에게 이자율, 수수료, 할인율, 가격, 마일리지, 서비스 등이 차별적으로 적용된다면 개인정보처리자의 정당한 차별화 전략에 따른 것이라도 양립성이 부정될 수 있다. 이 경우 "정보주체"란 해당 개인정보에 의해서 식별될 수 있는 모든 자를 의미하므로 제3자도 포함된다. 예컨대, SNS에 업로드된 단체사진, 게시판 메모 등의 경우 사진을 올리거나 메모를 쓴 사람뿐만 아니라 함께 사진을 찍은 동료 및 댓글을 달거나 "좋아요"를 누른 사람들의 이익도 고려해야 한다.

7. 보호조치 또는 보호수단의 유형 또는 종류

GDPR은 양립성 평가시 암호화 또는 가명화를 포함하여 적절한 보호수단의 존재 유무를 고려하도록 규정하고 있다. 적절한 보호수단으로는 암호화, 가명화, 익명화, 총계화, 침투 테스트 등과 같은 기술적 조치는 물론, 선택권(거부권)의 보장, 알고리즘 원리의 공개 및 설명, 양립성 평가결과의 공개, 추가 목적의 고지·공개 등 정보주체의 권리를 보호하기 위한 합리적인 모든 보호조치가 포함된다. 그 밖에 다양한 대안적 수단들도 보호수단에 포함된다. 이처럼 GDPR에서는 보호수단이 가명처리와 같은 기술적 조치나 침투 테스트와 같은 보안조치에 한정되지 않는다. 이에 반해 우리나라 개인정보 보호법 시행령 개정안과 신용정보법은 보호수단을 가명처리로 한정하고 있다.

8. 목적외 이용·제공 및 스팸 전송 목적의 개인정보 처리

GDPR에서는 계약 체결 및 이행, 개인정보처리자의 정당한 이익 추구 등이 추가처리의 주된 목적 중 하나이고, 광고성 정보(스팸)도 일정한 범위에서 추가처리를 허용하며, 가명정보도 이용·제공의 목적이 통계작성, 과학적 연구, 공익적 기록보존 등으로 제한되어 있지 않다. 그러나 개인정보 보호법은 계약 체결 및 이행과 개인정보처리자의 정당한 이익 추구를 목적으로 개인정보를 목적 외로 이용·제공할 때에도 정보주체의 동의를 받도록 규정하고 있고(제18조), 거래관계가 있는 동종의 상품에 대한 광고성 정보 전송의 경우에도 개인정보 수집·이용에 대한 동의를 받도록 요구하고 있으며, 가명정보의 이용·제공의 범위를 제한하고 있다. 양립성 규정의 도입으로 이들에 대해서도 추가처리가 가능한 것으로 적극적인 해석이 가능해 보인다.

9. 고려요소들 간의 상호 관계 설정의 문제

GDPR에서는 다섯 가지 고려요소들이 상호 보완적 또는 보충적 관계임과 동시에 상호 의존적관계에 있는 것으로 보고 있다. 즉 다섯 가지 고려요소들은 “복합적 고려사항(multi-factor assessment)”일 뿐 모든 고려사항을 빠짐없이 준수해야 하는 “필수 준수 요건”은 아니다. 따라서 하나의 고려요소를 충족하지 못한 경우 다른 고려요건을 통해서 그 결점을 보완할 수 있다. 이에 반해 개인정보 보호법 시행령 개정안(입법예고안)은 네 가지 고려요소를 모두 충족하도록 필수 요건으로 규정하고 있어 위임입법의 한계를 벗어난 것이 아닌지 의심을 받고 있다. 반면, 신용정보법은 4가지 요소를 고려하도록 규정하고 있다.

Ⅸ. 맺음말 : 양립성 평가의 한계

우리나라 개인정보 보호법 제15조제3항과 제17조제4항에 신설된 양립성 규정은 GDPR 제6조제4항을 벤치마킹한 것으로 볼 수 있으나 내용면에서 많은 차이가 존재함을 알 수 있다. GDPR은 보호와 활용을 균형있게 다루고 있는 반면, 국내법은 한편으로는 개인정보의 활용을 촉진하고자 하는 것 같으면서도 다른 한편으로는 개인정보의 활용을 제한하고 있어 그 정확한 의도를 파악하기 어렵다. 즉 현행 양립성 규정은 남용의 소지(특히 신용정보법)와 불용의 소지(특히 개인정보 보호법 시행령 개정안)를 둘 다 가지고 있다. 의도하지 않은 것이라면 GDPR의 양립성 규정을 입법자가 충분히 이해하지 못했던 부분이 있었던 것으로 보이고, 의도한 것이라면 양립성 규정의 취지를 제대로 살리기 어려울 것으로 보입니다. 양립성 규정이 개인정보처리자와 정보주체 모두에게 유용한 제도로 정착하기 위해서는 남용의 가능성을 최소화하면서도 유명무실한 조항으로 전락하지 않도록 유연한 해석이 필요해 보인다.

또한, 양립성 규정은 어디까지나 개인정보의 적법처리원칙에 대한 예외규정에 해당한다. 따라서 양립성 평가를 통한 개인정보의 추가처리에는 분명한 한계가 존재한다. 다섯 가지 양립성 평가요소를 종합적으로 평가하여 양립 가능하다고 판단되면 추가처리가 가능하나, 현실적으로 양립성을 모두 충족하는 것은 쉽지 않다. 뿐만 아니라 양립성의 판단기준 자체도 구체적이지 않고 애매하다. 따라서 WP29는 양립성 평가 결과가 의심할 여지없이 명확한 경우가 아니면, 정보주체로부터 자유롭고, 구체적이고, 명시적인 동의를 받거나 완전한 익명화 또는 총계화를 권장하고 있다. 또한, 양립성 평가가 철저히 이루어진 경우에도 추가적인 보호조치의 하나로 개인정보 영향평가를 권장한다.[55] 양립성 평가의 실패는 곧 법위반이 되어 고액의 과징금으로 이어질 수 있기 때문이다.

55) 29WP, 앞의 의견서, pp.36-37

〈참고문헌〉

1. Cédric Burton(May 15, 2013), European Regulators Opinion on "Purpose Limitation" Principle – What Constitutes "Compatible Use" in the Context of Big Data? https://www.wsgrdataadvisor.com/2013/05/
2. Monica Iancu & Vasile Soltan(February 10, 2020), Compatibility of purpose for further processing of personal data: hit the bull's eye in darts or hit the ball in a rugby gate? https://www.lexology.com/library/detail.aspx?g
3. 29WP, Opinion 03/2013 on Purpose Limitation, 2 April 2013 https://ec.europa.eu/justice/article-29/documentation/
4. WP29, Guidelines on Consent under Regulation 2016/679, 10 April 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
5. Wouter Seinen, Andre Walter & Sari van Grondelle(14 February 2019), Compatibility as a Mechanism for Responsible Further Processing of Personal Data. https://www.bakermckenzie.com/en/insight/publications/2019/02/
6. An official EU website, [Q&A] Can we use data for another purpose? https://ec.europa.eu/info/law/law-topic/data-protection/reform/
7. ICO, What is a 'compatible' purpose? https://ico.org.uk/for-organisations/guide-to-data-protection/

미국 음식배달 플랫폼 동향

이 경 남*

1. 개요

비대면(Untact)서비스에 대한 수요가 증가하면서 음식배달 서비스 시장이 급격히 확대되고 있다. 기존의 배달에 용이한 음식 위주의 서비스에서 확장하여 다양한 메뉴의 프랜차이즈 음식점 확충, 소비자 마케팅을 통한 수요 확대, 배달원 조직화 등 이해관계자들의 접점이 플랫폼을 중심으로 조율되면서 기존 서비스 영역을 확대해나가고 있다. 본고에서는 최근 미국을 중심으로 진행되고 있는 음식배달 사업자 동향을 분석하고 시사점을 제안한다.

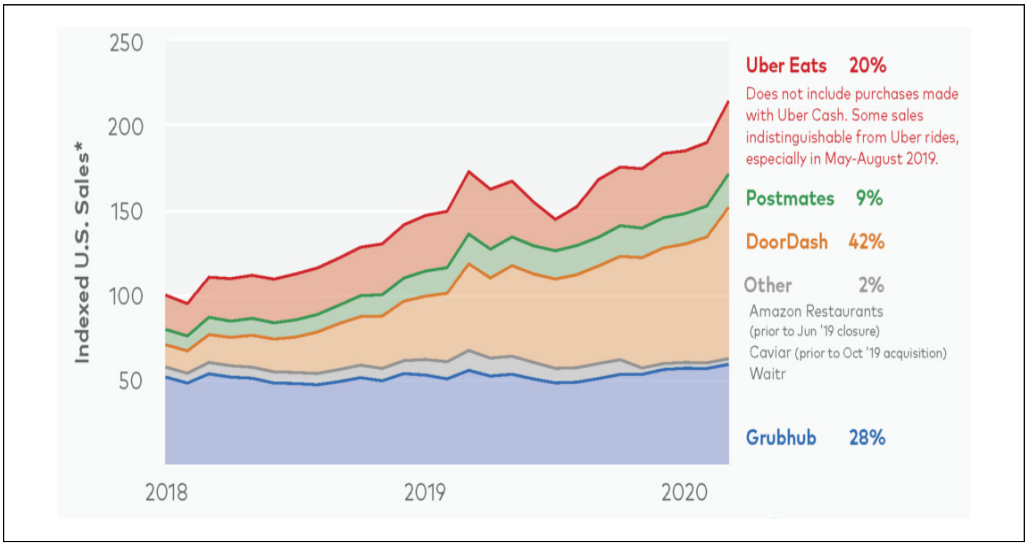
2. 미국 음식배달 서비스 동향

미국 음식배달서비스 시장은 2020년 3월 기준 전년동기대비 24% 성장한 것으로 조사되었다. 미국인의 약 28%가 배달서비스를 통해 음식을 주문하였는데 이는 작년의 22%에 비해 6%p 성장한 것이다(Rieck, 2020. 4. 21).

2020년 3월 기준 미국 3대 음식배달업체는 도어대시(DoorDash), 그럽허브(Grubhub), 우버잇츠(UberEats)로 각각 미국 음식배달 시장의 42%, 28%, 20%를 점유하고 있어 전체 음식배달시장의 90%를 차지하고 있다.

* 정보통신정책연구원 ICT전략연구실 부연구위원, (043)531-4287, knlee@kisdi.re.kr

[그림 1] 음식 배달 사업자 월별 매출액 추이

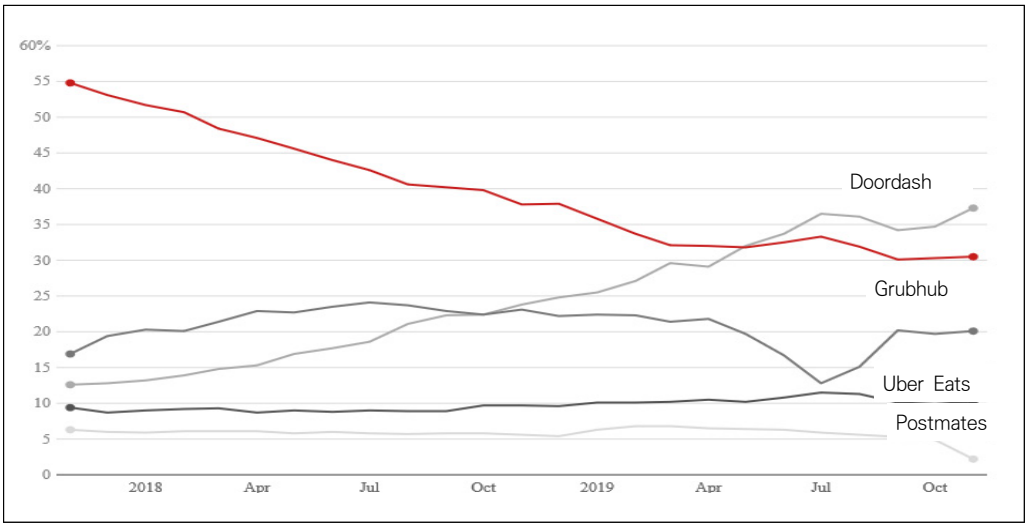


주: 2018년 1월 기준(=100) 음식 배달 매출액 Index, 2020년 3월 기준 점유율
자료: Second Measure, Rieck(2020. 4. 21)

이들 기업의 점유율 추이를 보면 2017년 11월 기준 그럽허브(Grubhub)가 55%의 시장을 점유하고 있었으나, 지속적으로 하락하여 2019년 1월 기준 36%, 2020년 3월 기준 28%로 하락하였다. 반면, 도어대시(DoorDash)는 2017년 11월 기준 13%에서 2019년 1월 기준 26%, 2020년 3월 기준 42%로 3위 사업자에서 1위 사업자로 급상승하였다. 우버이츠(Uber Eats)는 17~20%의 시장을 꾸준히 점유하고 있는 가운데 3개 업체의 음식배달 시장에서의 점유율은 85%에서 90%로 증가하였다.

[그림 2] 음식 배달 사업자 월별 매출액 추이

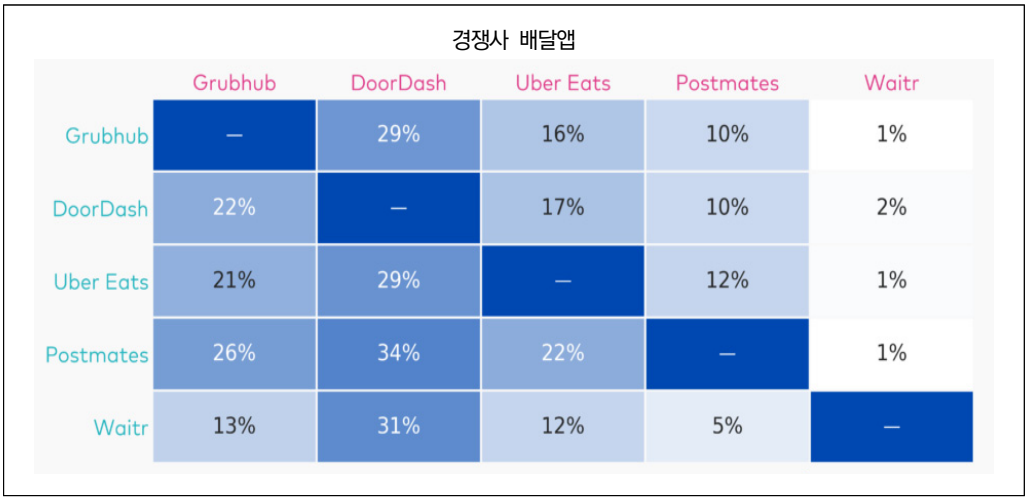
(단위: %)



주: Grubhub 데이터는 Seamless, Eat24의 데이터를 포함한 수치, Uber Eats는 2019년 5월 이후 자료의 경우 Uber rides와 구분이 어려워서 상기 수치보다 높은 점유율을 보일 수 있음

자료: Second Measure, Vox(2020. 1. 9)

[그림 3] 음식 배달 사업자간 중복 정도



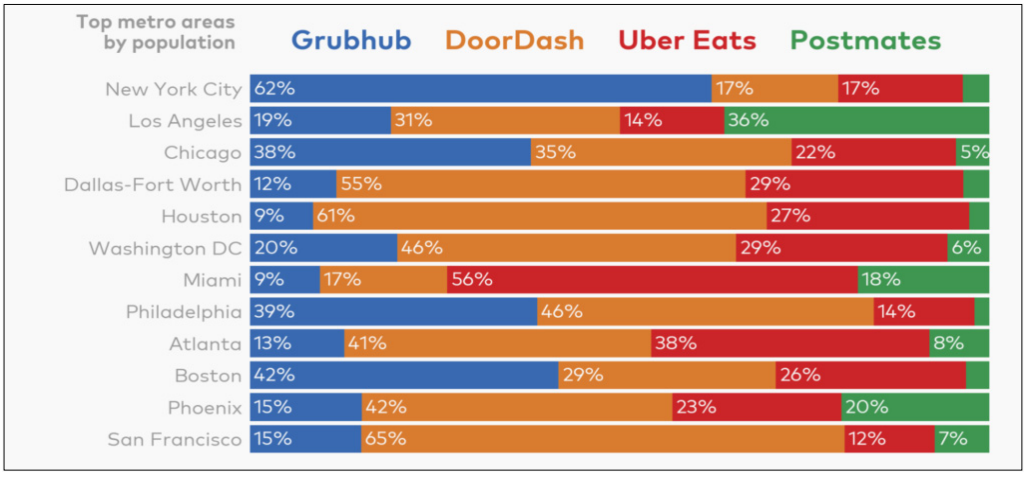
주: 2020년 1분기 기준 자사 배달앱 고객이 경쟁사 배달앱을 사용하는 비중

자료: Second Measure, Rieck(2020. 4. 21)

특히 음식배달서비스 시장은 여러 사업자가 음식 배달앱을 이용하는 것이 용이하고, 쿠폰 발행 및 마케팅 상황에 따라서 선택적으로 배달앱을 이용하는 멀티호밍(multi-homing) 비중이 매우 높다. [그림 3]을 보면 소비자가 경쟁 배달서비스 업체를 같이 이용하는 비중이 많게는 34%에 달하는 상황으로, 특히 포스트메이츠가 그 비중이 높아 취약한 상황이다.

이에 음식 배달서비스 업체들은 주력 지역을 중심으로 서비스를 전개하고 있는데, 그럽허브는 뉴욕과 보스턴, 우버잇츠는 마이애미와 애틀란타, 포스트메이츠는 LA를 중심으로 시장 점유율이 높다. 최근 점유율을 확대해나가고 있는 도어대시는 샌프란시스코, 휴스턴, 워싱턴 DC 등 다양한 지역에서 점유율을 높여나가고 있다([그림 4] 참조).

[그림 4] 지역별 매출액 비중



주: 2020년 3월 기준 지역별 매출액 점유율
자료: Second Measure, Rieck(2020. 4. 21)

미국의 음식배달서비스 시장은 최근 10년간 음식점, 소비자, 배달원 등 플랫폼 참여자를 최대한 확보하여 네트워크 효과를 극대화하기 위한 경쟁을 지속해왔다. 공급 측면에서는 참여자 유인을 높이기 위해 인기있는 프랜차이즈 음식점과의 (독점)계약 및 수익 배분률을 조정하였으며, 소비자에게는 할인 및 무료 배달 쿠폰 등을 제공하고, 배달원들에게는 배달 인센티브를 높게 책정하는 등의 공격적인 전략을 펼쳐왔다. 음식배달 서비스 업체들

은 이러한 경쟁 구도 속에서 대규모 적자를 보여왔으며, 그나마 10년만에 수익을 보였던 그럽허브도 최근 시장점유율 및 수익성이 떨어지고 있다.

이러한 상황에서 미국 음식배달서비스 업체들은 수익성 제고를 위한 노력 및 인수합병 등을 모색하고 있다. 음식점과의 제휴 확대로 배달 플랫폼이 음식점 검색의 일차적인 루트로 활용되면서 광고 수익 및 배달 수수료를 조정해 나가고 있으며, 소비자에게는 정기 구독 수수료 모델을 도입하여 안정적인 수익성을 확보하려는 시도와 함께 음식 도착 시간, 이동 상황 등에 대한 경로를 실시간으로 제시하거나 코로나 대응 비대면 전달, 개인화된 서비스 제공 등 차별화된 혜택을 제공하기 위해 노력하고 있다.

3. 결어

음식 배달서비스 플랫폼은 공급자(음식점)에게는 배달 서비스 운영을 외부화함으로써 비용을 절감하는 효과를 가져다주는 한편, 기존 소규모 배달업을 확장하여 규모의 경제를 가져오는 상호보완적인 비즈니스 모델로 시작하였다. 미국의 경우 비교적 먼 배달 거리 및 높은 인건비 등의 제약하에서 플랫폼이 배송 시간 및 경로 최적화 등을 통해 기존 배달의 비효율성을 제거함으로써 공급자와 소비자에게 혜택을 제공하면서 성장하였다.

다만, 음식배달서비스의 경우 이렇게 구축된 초기 선점 효과가 사업자간 높은 멀티호밍으로 인해 안정적으로 유지되지 못하고 있어 수익성 확보에 어려움을 겪고 있다. 최근 1위 사업자였던 그럽허브의 점유율 및 수익이 하락한 것도 이러한 맥락에서 해석될 수 있으며, 이에 따라 배달서비스 업체를 둘러싼 인수합병이 지속되고 있다.

이와같이 플랫폼 비즈니스 모델은 네트워크 효과를 극대화하기 위해 초기에는 다면 시장의 이용자 규모 확대에 주력하였지만, 멀티호밍이 높은 비즈니스 영역에서는 가격 프로모션 및 마케팅 경쟁 속에서 소비자를 최대한 고착화하기 위한 차별적인 혁신 서비스(ex, 개인화된 음식 추천, 시간대, 패턴) 제공이 필수적이며, 적정 사업자수로의 수렴이 진행되는 것이 특징이다.

〈참고문헌〉

Rieck(2020. 4. 21.), Which company is winning the food delivery war?.

Vox(2020. 1. 9.), “Grubhub sale rumors highlight the state of the struggling food-delivery industry”.

Choudary(2020. 3. 17.), The economics of food delivery platforms: What’s good for the platform is bad for the ecosystem.