전자상거래에서의 개인정보 처리

I. 들어가는 말

II. 전자상거래 기업에 있어서의 개인정보의 처리: 적용 법령을 중심으로

III. 전자상거래 산업에 있어서의 개인정보의 처리: Life Cycle 관점에서

1. 수집
2. 이용
3. 제3자 제공 / 위수탁
4. 가명정보와 익명정보
5. 보관 / 파기 및 기타 정보보호의무

IV. 전자상거래에 있어서 개인정보 관련 몇 가지 쟁점

1. 전자금융거래와 개인(신용)정보
2. 마이데이터 / 개인신용정보 전송요구권과 전자상거래
3. 전자상거래 등에서의 소비자보호에 관한 법률
4. 맞춤형 광고와 행태정보의 수집
5. 온라인 플랫폼 중개거래의 공정화에 관한 법률

V. 맺음말

손도일
법무법인 율촌 파트너
변호사

I. 들어가는 말

COVID-19 이전에도 전자상거래 등 비대면거래의 활성화는 진행되고 있었지만, COVID-19 이후 폭발적으로 확대되었고, 이와 같은 변화는 가속화될 것으로 보인다. 마침 2020. 1. 9. 데이터 3법이라고 불리는 「개인정보 보호법」("개인정보법"), 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」("정보통신망법"), 「신용정보의 이용 및 보호에 관한 법률」("신용정보법")이 국회를 통과하여 2. 4. 공포되고 8. 5.부터 시행됨에 따라("데이터 3법 개정"), 전자상거래 산업에 있어서 개인정보의 활용과 보호의 필요성은 그 어느 때보다 크게 되었다.

특히 데이터 3법의 개정으로 가명정보 등의 개념을 도입하고, 일정한 범위·요건 하에서 별도의 동의 없이도 개인정보를 기존의 수집 목적 범위 이외의 목적으로도 이용 또는 제공("개인정보의 추가적 이용 또는 제공")할 수 있는 등 개인정보의 활용 범위가 상당한 정도로 확대되었다. 한편, 인공지능을 포함한 기술의 발전과 함께 개인정보를 활용할 수 있는 사업모델도 크게 확대되어, 이제는 전자상거래를 통하여 수집되는 개인정보의 중요성은 더욱 커지게 되었다.

이하에서는 전자상거래 산업에 있어서 개인정보의 수집부터 파기까지의 전체적인 생애주기(life cycle) 관점에서 개인정보의 처리 관련 주요 사항에 관하여 살펴보고자 한다.

II. 전자상거래 기업에 있어서의 개인정보의 처리: 적용 법령을 중심으로

전자상거래 기업은 정보통신망을 이용하여 그 서비스를 제공하는 기업이므로 정보통신망법 소정의 정보통신서비스 제공자에 해당하고,[1] 해당 기업의 개인정보의 처리[2]에 대하여는 주로 개인정보법이 적용된다.[3] 특히 개인정보법 제39조의 3 이하 "제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례" 규정("특례규정")이 우선적으로 적용되고, 정보통신망법상의 일부 규정도 적용된다. 한편, 개정 전 정보통신망법에 따라서 정보통신서비스 제공자에게 적용되었던 개인정보처리에 관한 규정들은 개인정보법 제6장의 특례규정으로 이전되면서 개인정보법에 통합되었다. 따라서 동일한 사안에 적용될 수 있는 일반규정과 특례규정이 모두 존재하고 또한 그 내용 간에 충돌이 있는 경우에는 특례규정이 적용된다. 그러나 일반규정에만 존재하는 사항에 대하여는 일반규정이 함께 적용된다.[4]

한편, 개인정보의 또 다른 한 축이라고 할 수 있는 개인신용정보[5]의 경우에는 신용정보법이 우선적으로 적용되지만, 데이터 3법 개정 이전부터 신용정보법의 비금융기관에 대한 적용범위에 관하여는 논란이 있었고, 개정 이후에도 이 문제는 명확하게 정리되지 않은 것으로 보인다. 이는 개인정보보호위원회("보호위원회")와 금융위원회("금융위") / 금융감독원의 전자상거래 기업 및 보유 데이터에 대한 규제 권한과도 밀접한 관련이 있는 문제이다.[6]

1) "정보통신서비스 제공자"란 전기통신사업법 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다(정보통신망법 제2조 제1항 제3호).

2) 처리라 함은, 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다(개인정보법 제2조 제2호).

3) 정보통신망법 제5장 이하의 정보통신망에서의 이용자 보호에 관한 규정 및 제6장 이하의 정보통신망의 안정성 확보에 관한 조항들은 정보통신서비스 사업자인 전자상거래 기업에게 계속 적용된다.

4) 가령 가명정보의 활용에 관한 일반규정은 전자상거래 기업(즉, 정보통신서비스 제공자)에게도 적용이 된다.

5) 신용정보 중 개인신용정보라고 함은 기업 및 법인에 관한 정보를 제외한 살아있는 개인에 관한 신용정보로서 해당 정보만으로 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정개인을 알아볼 수 있는 정보도 포함된다(신용정보법 제2조 제2호). 한편 "신용정보"란 금융거래 등 상거래에서 거래 상대방의 신용을 판단할 때 필요한 정보로서 신용정보주체의 거래내용, 신용도 혹은 신용거래능력을 판단할 수 있는 정보를 말한다(신용정보법 제2조 제1호).

6) 신용정보의 이용 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 신용정보법에 정하는 바에 따르지만, 개인정보의 보호에 관하여는 신용정보법에 특별한 규정이 있는 경우를 제외하고는 개인정보법에서 정하는 바에 따라야 한다(신용정보법 제3조의2). 한편 개인정보법 제6조는 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보법에 따르도록 되어 있다. 한편 보호위원회는 '특별한 규정'으로 판단할 수 있는 기준으로 상호 모순 혹은 저촉되는 규정의 존재 여부, 개인정보법 관련 조항을 배제하고자 하는 내용의 포함 여부라고 결정한 바 있다(보호위원회 결정 제2018-02-006호). 그러나 이와 같은 규정 및 해석만으로는 신용정보법을 일반 기업에 어느 정도까지 적용할 것인지에 관하여 명확한 결론을 내리기는 어렵다. 이에 관하여는 신용정보의 개념에 관한 복잡한 논의가 필요한데, 이는 본 원고의 범위를 넘는 것이어서 추후 다른 기회에 논의를 하고자 한다.

개정 신용정보법의 기본적인 입장은 신용정보법의 일반 기업에 대한 적용을 전제로 하면서도, 대신 일반 기업들에 대한 신용정보법 관련 감독권을 보호위원회에 주려는 입장인 것으로 보인다. 즉, 신용정보법 제45조의3에 의하여, 보호위원회는 금융위의 감독을 받지 아니하는 신용정보제공·이용자("상거래기업")가 상거래기업이 "상거래정보보호규정"[7]을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우 혹은 그 위반에 대한 신고를 받거나 민원이 접수된 경우, 해당 상거래기업에게 관계 물품·서류 등 자료를 제출하게 할 수 있다.

이상의 점들을 종합적으로 해석한다면, (1) 전자상거래 기업에 대한 신용정보법 적용 범위에 대하여는 아직 명확한 해결이 되지 않은 것으로 보이고, (2) 신용정보법이 적용된다고 하더라도, 해당 기업들이 「금융위원회의 설치 등에 관한 법률」 제38조에 의하여 금융위의 검사를 받는 기업이 아니라면, 이에 대하여는 보호위원회가 상거래정보보호규정에 대한 감독권을 행사한다는 정도로 결론을 도출할 수 있을 것이다.

실무상의 혼란을 최소화하려면, 신용평가를 위하여 고객의 정보를 사용하지 않는 일반 전자상거래 기업에 대하여 신용정보법을 적용하는 것에 관하여는 보다 명확하게 입법으로 해결하는 것이 필요하다고 할 수 있다.

참고로 EU의 경우 개인정보와 신용정보를 우리 법제와 같이 명확하게 구분하고 있지는 않고 일반 개인정보보호 규정(General Data Protection Regulation; "GDPR")에서 전체적으로 규율하고 있고, 미국의 경우에는 공공기관에 대하여는 Privacy Act, 금융기관에 대하여는 Gramm-Leach-Bliley Act, Fair Credit Reporting Act 등 개별법을 통하여 각 산업별로 이를 규율하고 있다.[8]

III. 전자상거래 산업에 있어서의 개인정보의 처리: Life Cycle 관점에서

앞서 본 바와 같이 일반적인 전자상거래 기업에 대하여는 기본적으로 개인정보법이 적용되고, 그 개인신용정보의 활용 형태에 따라 신용정보법이 적용된다. 이하에서는 전자상거래와 개인정보 처리를 개인정보법을 중심으로 검토하되, 신용정보법과 차이가 중요한 부분에 대하여는 신용정보법의 내용을 함께 검토하기로 한다. 다만, 여러 산업에 공통되는 개인정보 관련 법령은 그 언급을 최소화하기로 하고, 여기에서는 전자상거래 특성에 따른 부분을 중심으로 기술하기로 한다.

1. 수집

전자상거래 기업의 경우 정보통신망을 이용하여 서비스를 제공하는 경우에는, 개인정보법 제39조의 3 이하 "제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례" 규정이 적용된다. 전자상거래 기업도 기본적으로 정보주체의 동의를 받아서 개인정보를 수집하는 것이 원칙이지만, 정보통신서비스의 제공에 관

7) 신용정보법 제15조 및 제17조 (개인신용정보의 수집, 처리 및 위탁), 제19조 및 제20조의2 (신용정보시스템의 안전, 개인신용정보의 보관기간), 제32조(제공활용동의) · 제33조(이용) · 제34조(개인식별정보) · 제36조(상거래거절근거고지) · 제37조(이용동의철회) · 제38조(열람정정청구) · 제38조의3(삭제요구) · 제39조의4(누설통지) · 제40조의2(가명·익명처리) 및 제42조(업무목적외 누설금지)를 말한다.

8) 박광배, "거래정보 및 (개인)신용정보의 활용과 보호", 핀테크시대, 박영사, 2016, 제223-224면

9) 참고로 전자상거래 기업이 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우에는 보호위원회는 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다(개인정보법 제39조의15 제1항 제6호). 또한 전자상거래 기업이 이를 위반한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다(개인정보법 제71조 제4의 5호). 또한 양벌 규정에 따라 기업 및 해당 위반행위를 한 자에 대하여 벌칙이 모두 적용된다(개인정보법 제74조).

10) 정보통신서비스를 제공하지 않는 일반적인 개인정보처리자의 경우, 정보주체(이용자)의 동의를 얻어서 개인정보를 수집하는 것이 가장 일반적이라고 할 수 있지만, 예외적으로 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우, 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우에는, 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우, 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우에도 동의없이 개인정보를 수집하는 것이 인정된다(개인정보법 제15조 제1항).

한 계약을 이행하기 위하여 필요한 개인정보로서 경제적 · 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 혹은 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우에도 동의 없이 개인정보를 처리할 수 있다(개인정보법 제39조의 3 제2항 제1호 및 제2호). 그러나 이와 같은 예외조항은 대부분의 전자상거래 기업들이 제공하는 서비스에 대하여는 적용의 여지가 적다고 할 수 있으므로, 전자상거래 실무상으로는 사전동의에 기반하여 개인정보를 수집하는 옵트인(opt-in) 방식이 보편적이라고 할 수 있다. 정당한 근거 없이 동의 없이 개인(신용)정보를 처리하는 경우의 제재가 워낙 중대하기 때문에 기업 입장에서는 동의에 기반하여 업무를 처리할 수 밖에 없다.[9)10)11)]

반면, GDPR은 정당한 이익(legitimate interest)에 기반한 개인정보처리를 우리나라에 비하여 보다 광범위하게 인정하고 있다.[12)]

전자상거래 기업이 개인정보 수집 동의를 받을 때에는, 개인정보의 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 정보주체에게 알려야 하고, 이를 변경하는 경우에도 이를 알리고 동의를 받아야 한다(개인정보법 제15조 제2항). 이중 동의거부권에 대하여는 정보통신서비스 제공자 등에 대한 특례를 정하고 있는 동법 제39조의 3 제1항에서는 이를 규정하고 있지 않으나, 이용자의 보호를 위하여 실무상 해당 조항을 동의서에 포함하도록 권장하고 있고,[13)] 대부분의 전자상거래 기업에서 쓰는 동의서 양식에도 해당 내용을 포함하고 있다. 한편, 고객(정보주체)으로부터 동의를 받는 경우에도 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다(동법 제22조 제1항). 이를 포괄동의의 금지원칙이라고 한다.[14)]

전자상거래의 특성상 인터넷 홈페이지나 전자우편 혹은 전화를 통하여 동의를 받는 경우가 대부분이고 이는 모두 가능하다(개인정보법 시행령 동법 시행령 제17조 제1항). 다만, 앞서 본 기본적인 수집항목(수집이용목적, 수집항목, 보유 및 이용기간, 동의거부권) 이외의 마케팅 목적 이용 동의, 민감정보, 고유식별정보, 제3자 제공 관련 내용 등 '중요한 사항'들은 다른 항목들과 구분하여 동의를 받되(동법 시행령 제17조 제2항), 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게하여야 하고, 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 하는 등 그 밖의 내용과 별도로 구분하여 표시하는 것이 필요하다(개인정보 처리 방법에 관한 고시(보호위원회 고시 제2020-7호, 제4조). 이를 위반하는 경우 그 동의의 효력 자체가 부정될 수 있다는 점에 유의하여야 한다(대법원 2016. 6. 28 선고 2014두2638 판결[15)16)] 참조).

과거 일부 전자상거래 기업은 고유식별정보를 과다하게 수집하는 경우가 있어서 문제가 되었다. 즉, 주민등록번호, 여권번호, 운전면허번호 및 외국인등록번호와 같은 고유식별정보는, 정보주체에게 별도의 동의를 받거나 법령에서 이

11) 신용정보법에서는 동의를 받지 않고 수집할 수 있는 예외로, 법령에 따라 공개된 정보, 출판물/방송매체/공공기관의 홈페이지에 공개된 정보, 정보주체가 스스로 SNS에 공개한 정보(단, 이 경우에는 동의가 있었다고 객관적으로 인정되는 범위 내로 한정)는 동의 없이 수집할 수 있는 것으로 규정하고 있다(신용정보법 제15조 제2항).

12) GDPR Article 6(1)(a)와(f)에 의하면 Data Processing은 동의가 있거나 아니면 개인정보처리자(data controller) 혹은 제3자의 정당한 사유(legitimate interest)가 있는 경우에도 가능하다. 다만 정보주체의 권리와 자유가 근본적으로 더 중요한(overridden) 경우에는 그러하지 아니하다(특히 정보주체가 아동인 경우)고 규정하고 있다. 한편, 정당한 사유는 Recital 47조에서 fraud 예방이나 Direct Marketing에서 인정되는 것으로 보고 있다. 또한 Recital 48조에서는 개인정보처리자가 Group 중 하나인 경우 고객 혹은 임직원의 개인정보를 내부 행정 목적으로 제공하는 것도 인정하고 있다. Recital 49조에서는 정보통신망 안전을 위하여 불법적인 접근을 막기 위하여 개인정보를 처리하는 것도 인정하고 있으며, Recital 50조에서는 당국에 불법적인 행동이나 위험을 통보하기 위하여 개인정보를 처리하는 것도 정당한 사유에 해당하는 것으로 보고 있다.

13) 개인정보보호위원회, 개인정보 보호법령 및 지침·고시 해설(2020. 10. 6.자 사전공개 초안), 2020, 416면.

14) 여기서 각각의 동의를 받아야 하는 사항이라고 함은, 수집·이용 동의(제15조 제1항 제1호), 제3자 제공 동의(제17조 제1항 제1호, 제39조의 3 제1항), 국외 제3자 제공 동의(제17조 제3항), 마케팅 목적 처리 동의(제22조 제4항), 법정대리인의 동의(제22조 제6항) 등이 있다. 한편, 개인정보처리자는 정보주체가 다른 개인정보처리의 목적과 '별도로' 동의 여부를 표시할 수 있도록 조치를 취하고 동의를 받아야 하는 경우가 있다. 이는 정보주체의 보다 신중한 선택을 요구하는 항목이라고 할 수 있다. 이에는 목적 외 이용·제공 동의(제18조 제2항 제1호), 개인정보를 제공받은 자의 이용·제공 제한(제19조 제1호), 민감정보 처리 동의(제23조 제1항 제1호), 고유식별정보 처리 동의(제24조 제1항 제1호) 등이 해당된다. 예컨대, 고유식별정보(주민등록번호 제외)를 수집할 때에는 「고유식별정보 수집·이용·제공에 대한 동의」를, 건강정보에 관한 정보를 수집할 때에는 「건강정보(민감정보) 수집·이용·제공에 대한 동의」를 별도로 분리해서 목적 등을 고지하고 동의를 받아야 한다. [개인정보보호위원회, 앞의 책, 147면]

를 허용하는 경우에만 처리할 수 있다(개인정보법 제24조). 특히 주민등록번호는 법령에서 허용되지 않는 경우가 아닌한 주민등록번호를 수집할 수 없다(개인정보법 제24조의 2). 일부 전자상거래 기업의 경우, 로그인 인증수단으로 안면인식이나 지문인식을 쓰고 있는데, 이와 같은 정보들은 민감정보이므로 별도의 동의를 받아야 한다(동법 시행령 제18조). 이와 같이 합법적으로 수집한 민감정보나 고유식별정보에 대하여는 안전성확보에 필요한 조치를 취하여야 하며, 특히 고유식별정보에 대하여는 암호화등의 추가적인 안전성 확보조치를 취하여야 한다(동법 제23조 및 제24조, 동법 시행령 제21조 및 제22조).

한편, 전자상거래에 있어서는 미성년자 여부를 식별하는 것이 그 거래의 안정성을 담보하기 위하여 필요한데, 특히 만 14세 미만 아동의 개인정보를 처리하기 위하여 개인정보 처리에 관한 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다(동법 제39조의 3 제4항 및 제5항). 다만, 이때 수집한 법정대리인의 개인정보는, 해당 아동의 법정대리인으로서의 동의를 얻기 위한 목적으로 사용되어야 하며, 동의거부가 있거나 동의의사를 확인할 수 없었던 경우에는 수집일로부터 5일 내에 파기하도록 권고된다(표준 개인정보 보호지침 제13조).

전자상거래에 있어서 기업들은 가급적 거래가 이루어진 후에라도 계속하여 마케팅 활동 등을 통하여 그 관계를 지속하여 나가려고 하는 경향이 강한데, 정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보[17] 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부할 수 없다는 데 유의하여야 한다(동법 제39조의3 제3항).

전자상거래 기업이 개인정보를 공개된 데이터베이스(DB)나 홈페이지로부터 수집하여 이를 활용하려고 하는 경우가 있다. 일단 공개된 개인정보를 수집함에 있어서는 해당 정보주체의 개인정보자기결정권 내지 프라이버시권, 다른 기업(즉 공개된 DB 소유자)의 권리 등을 종합적으로 고려하여야 한다. 이에 관한 리딩케이스라고 할 수 있는 대법원 2016. 8. 17 선고 2014다235080 판결에서는 (1) 이미 공개된 개인정보를 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내에서 수집 · 이용 · 제공 등 처리를 할 때는 정보주체의 별도의 동의는 불필요하고, (2) 정보주체의 동의가 있었다고 인정되는 범위 내인지 여부는 공개된 개인정보의 성격, 공개의 형태와 대상 범위, 그로부터 추단되는 정보주체의 공개 의도 내지 목적뿐만 아니라, 정보처리자의 정보제공 등 처리의 형태와 정보제공으로 공개의 대상 범위가 원래의 것과 달라졌는지, 정보제공이 정보주체의 원래의 공개 목적과 상당한 관련성이 있는지 등을 검토하여 객관적으로 판단하여야 하고, (3) 국민 누구나가 일반적으로 접근할 수 있는 정보원(情報源)에 공개된 개인정보의 경우에는 이를 수집할 수 있는 '알 권리'가 정보처리자나 그로부터 정보를 제공받는 정보수용자에게 인정됨은 물론, 이러한 '알 권리'를 기반으로 하는 정보수용자들의 표현의 자유도 이 사건 개인정보의 처리행위로 보호받을 수 있는

15) 동 판결은 이 사건 이벤트 화면에서 법정 고지사항을 제일 하단에 배치한 것, 이 사건 이벤트 화면에 스크롤바를 설치한 것만으로는 법정 고지사항이 존재한다는 점을 쉽게 인지하여 이를 확인할 수 있는 형태라고 볼 수 없는 점, 이 사건 이벤트 화면에서 그 팝업창 문구 자체만으로는 수집 · 제공의 대상이 '개인정보'이고 제공처가 제3자인 보험회사라는 점을 쉽고 명확하게 밝힌 것으로 볼 수 없음에도, 이용자가 팝업창에서 '확인'버튼만 선택하면 개인정보 수집 · 제3자 제공에 동의한 것으로 간주되도록 한 점 등을 이유로 동의의 효력을 부정하였다.

16) 또한 대법원은 2017. 4. 7 선고 2016도13263 판결(위에서 본 2014두2638 판결과 같은 사실관계에서 파생된 형사사건이다)에서도 사안을 종합적으로 고려하여 동의가 효력이 없다고 판단하였다.

- 이 사건 경품행사의 목적은 처음부터 고객들의 개인정보를 수집하여 이를 보험회사에 대가를 받고 판매하는 데 있었음. 이 사건 경품행사를 진행하면서 위와 같은 목적을 은폐하고 광고한 것은 '표시 · 광고의 공정화에 관한 법률' 위반임
- 이 사건 응모권에 따라서는 경품추첨 사실을 알리는 데 필요한 개인정보와 관련 없는 '응모자의 성별, 자녀 수, 동거 여부' 등 사생활의 비밀에 관한 정보와 심지어는 주민등록번호와 같은 고유식별정보까지 수집하였음
- 더욱이 이 사건 경품행사를 위하여 사용된 응모권에 기재된 동의 관련 사항은 약 1mm 크기의 글씨로 기재되어 있어 소비자의 입장에서 보아 그 내용을 읽기가 쉽지 않음.

17) 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.

법적 이익에 포함된다고 볼 수 있다고 판시한 바 있다.[18)]

한편, 이와 같이 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 개인정보의 수집 출처, 개인정보의 처리 목적, 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 정보주체에게 알려야 한다(개인정보법 제20조 제1항). 단, 개인정보처리 규모가 큰 대규모 정보처리자일 경우[19)]에는(대형 전자상거래 기업은 대부분 이에 해당한다), 서면·전화·문자전송·전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 개인정보를 제공받은 날부터 3개월 이내에 (정보주체의 요구가 없다고 하더라도) 정보주체에게 알려야 한다.

2. 이용

전자상거래 기업의 경우 동의를 받은 목적 범위 내에서 개인정보를 활용하는 것이 원칙이다(개인정보법 제39조의3 제1항). 다만, (1) 정보통신서비스 제공자에 대한 특례 규정에 따라 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적, 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우, (2) 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우, (3) 다른 법률에 특별한 규정이 있는 경우에 한하여 그 동의가 없더라도 이용자의 개인정보를 수집, 이용할 수 있다(같은 항 제2항)는 점은 앞서 "수집"에서 본 바와 같다.

한편, 2020. 2. 데이터 3법 개정 전에는 예외 사유에 해당하지 않는 한 기존 동의서의 내용과는 다른 내용으로 개인정보를 이용하는 것은 허용되지 않았다. 그러나 이에 관하여는 최초 동의서를 수집할 당시에 해당 기업이 미래의 모든 상황을 예상한다는 것은 불가능하고, 사실상 새로운 동의를 기존 고객들로부터 받는 것은 그 회신율이 매우 저조한 점을 고려할 때 기업에는 큰 부담이 되어왔던 것도 사실이다. 특히 새로운 사업모델의 개발빈도가 높은 전자상거래 기업의 경우에 이와 같은 문제가 많았다.

이번 데이터 3법 개정을 통하여 이와 같은 불편을 해소하고자 일정한 요건을 갖추면, 개인정보처리자(전자상거래 기업 포함)는 개인정보를 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령[20)]으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용하고(개인정보법 제15조 제3항), 제3자에게 제공도 할 수 있게 되었다(동법 제17조 제4항). 한편 신용정보법도 유사한 추가적인 이용·제공 기준을 제시하고 있는데, 문언상으로만 보면 신용정보법의 기준이 좀더 완화된 것으로 볼 여지가 있어서, 개인신용정보를 함께 다루는 경우가 많은 전자상거래 기업 입장에서는 혼란스러울 수도 있다. 그러나 실제적인 차이는 문언상의 차이만큼은 크지 않을 것으로 예상하고 기대한다. 기본적으로 두 법상의 조항 모두 사전동의를 원칙으로 하는 제도의 일부 문제점

18) 본 사안은 원고인 대학교수의 개인정보를 피고 기업이 수집하여 이를 유료로 제공한 사안이다. 이에 대하여 대법원은 법률정보 제공 사이트를 운영하는 피고 기업이 A대학 법학과 교수로 재직 중인 원고의 사진, 성명, 성별, 출생연도, 직업, 직장, 학력, 경력 등의 개인정보를 위 법학과 홈페이지 등을 통해 수집하여 위 사이트 내 '법조인' 항목에서 유료로 제공한 사안에서, 피고 기업의 행위를 원고 교수의 개인정보자기결정권을 침해하는 위법한 행위로 평가하거나, 피고 기업이 개인정보 보호법 제15조나 제17조를 위반하였다고 볼 수 없다고 판시하였다.

19) 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자 혹은 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자

20) 정보주체의 동의 없이 개인정보를 추가적으로 이용 또는 제공하려는 경우에는 당초 수집 목적과 관련성이 있는지 여부, 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부, 정보주체의 이익을 부당하게 침해하는지 여부, 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부를 고려하여야 한다(개인정보법 시행령 제14조의 2 제1항)

을 합리적인 한도에서 해소하려는 목적으로 만들어진 것이라는 점에서는 공통된 점이 있고, 그 추가적인 이용범위를 합리적으로 제한하여야 한다는 점에서도 그 궤를 같이 하기 때문이다.

3. 제3자 제공 / 위수탁

전자상거래 기업은 정보주체의 동의를 받은 경우 혹은 법률의 특별한 규정이 있거나 법령상의 의무를 준수하기 위하여 불가피한 경우에는 개인정보를 제3자에게 제공할 수 있다(개인정보법 제17조 제1항, 제18조 제1항 및 제2항).[21)22)]

전자상거래 기업들 중에서는 실무상 동의를 받을 당시의 개인정보를 제공받는 제3자가 너무 많은 경우에 링크(link)를 통하여 게시하는 경우가 있다. 현실적으로 동의서에 이를 다 표시하는 것이 어렵다면 이와 같은 방법이 위법하다고 보기는 어렵다. 실무에서 가장 문제가 되는 부분은 그룹에 속한 회사들이 그룹 계열사들과 직원들의 개인정보 내지 고객들의 개인정보를 공유하는 경우, 동의 당시의 계열 회사에 변동이 생기는 경우이다(합병 등으로 새로운 회사가 되거나 새로운 회사가 추가되는 경우). 이 경우에는 원칙적으로 동의를 새로이 받는 것이 원칙이지만, 앞서 본 바와 같이 당초 수집 목적과의 합리적 관련성 등을 기준으로 판단하여 합리적인 범위 내에서의 추가적인 이용도 가능하다고 해석된다(동법 제17조 제4항).

특히 다국적 전자상거래 기업 내지 해외 업체들과 거래가 많은 전자상거래 기업의 경우, 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다) · 처리위탁 · 보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다(동법 제39조의12 제1항 본문). 즉, 일반 개인정보처리자는 국외 "제3자 제공"의 경우에만 정보주체의 동의를 필요로 하지만, 전자상거래 기업은 위탁과 보관의 경우에도 이용자의 동의를 받는 것을 원칙으로 하였다. 다만, 이전되는 개인정보 항목, 이전되는 국가, 이전일시 및 이전방법, 이전받는 자의 명칭(정보관리책임자 연락처 포함), 이전받는 자의 이용목적 및 보유·이용 기간을 개인정보처리방침에 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다(동조 1항 단서). 이와 같은 특례는 위탁·보관에만 적용되는 것이고 제3자 제공에는 적용되지 아니하므로, 제3자 제공시에는 별도로 동의를 받아야 하는 점에 유의하여야 한다.

한편, 이용자의 개인정보를 이전받는 자가 해당 개인정보를 제3국으로 다시 이전하는 경우에 관하여는 별도로 동의를 받거나 위와 같은 방법에 따라 공개·고지하여야 한다(동조 제5항). 가령 한국 자회사가 미국 본사에 정보를 이전한 후 미국 본사가 유럽의 다른 계열사에 해당 정보를 제3자 제공하는 경우에는 별도의 동의가 있어야 한다.

한편 제3자 제공과 구별되는 개념으로 개인정보의 위탁·수탁이 있다. 제3자

21) 한편, 정보통신서비스 제공자가 아닌 일반 개인정보처리자는 정보주체 또는 그 법정대리인으로부터 사전동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정하는 경우에도 개인정보를 목적 외로 이용하거나 제3자에게 제공할 수 있다(개인정보보법 제18조 제2항).

22) 개인정보처리자가 개인정보를 정보주체로부터 별도의 동의를 받거나 법률의 규정에 따라 당초 동의 범위를 넘어서서 제공하는 경우에는, 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하고, 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다(개인정보법 제18조 제5항). 한편, 제3자 제공을 받은 자는 정보주체로부터 별도의 동의를 받거나 법률의 다른 규정이 없는 한, 해당 개인정보를 제공받은 목적 이외의 용도로 사용하거나 다른 제3자에게 제공을 할 수 없다(개인정보법 제19조).

제공이 개인정보를 제공받는 자의 이익을 위하여 이루어지는 것이라면, 위탁은 제공하는 자(위탁자)의 이익을 위하여 이루어지는 것이다. 최근 광범위하게 사용되는 클라우드 서비스의 경우, 클라우드 서비스 제공자들은 별도로 해당 개인정보에 접근할 수 없는 경우가 일반적이므로, 클라우드 서비스 이용자는 위탁자이고 동 서비스 제공자는 수탁자가 된다. 그러나 전자상거래업체들이 그들이 보유한 빅데이터의 분석을 제3자에게 의뢰한 경우, 해당 데이터를 분석을 의뢰한 전자상거래 업체 이외에도, 해당 분석기업 자체의 이익을 위하여도 사용할 수 있다면 이는 제3자 제공과 위탁이 혼재된 경우이고, 이 경우에는 제3자 제공요건 뿐만 아니라 위탁에 요구되는 별도의 요건을 모두 충족하여야 한다.

실무적으로는 이와 같이 제3자 제공과 위탁이 혼합된 경우가 많다고 할 수 있으며, 어떠한 행위가 개인정보의 제공인지 아니면 처리위탁인지는 개인정보의 취득 목적과 방법, 대가 수수 여부, 수탁자에 대한 실질적인 관리·감독 여부, 정보주체 또는 이용자의 개인정보 보호 필요성에 미치는 영향 및 이러한 개인정보를 이용할 필요가 있는 자가 실질적으로 누구인지 등을 종합하여 판단하여야 한다(대법원 2017. 4. 7 선고 2016도13263 판결).[23]

개인정보를 위탁하는 경우에는, 위탁업무의 내용과 수탁자를 위탁자의 인터넷 홈페이지에 지속적으로 게재하는 방법으로 정하는 방법에 따라 공개하여야 한다(개인정보법 제26조 제1항, 제2항, 동법 시행령 제28조 제1항 및 제2항).[24]

전자상거래 기업의 경우, 계약의 이행을 위한 업무 위·수탁의 경우보다는 마케팅 목적의 위·수탁의 경우에 개인정보의 보호문제가 더 중요하게 대두된다. 전자상거래 기업이 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는, 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다(개인정보법 제26조 제3항, 동법 시행령 제28조 제4항). 단, 위탁자가 과실 없이 이와 같은 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다(동법 시행령 제28조 제5항).[25]

위탁의 경우에는 원칙적으로 정보주체의 동의를 필요로 하지 않지만, 대신 위탁자는 수탁자의 정보처리에 대한 감독의무가 있다. 수탁자의 법 위반행위에 대하여는 위탁자도 함께 책임을 진다(개인정보법 제26조 제4항 내지 제6항). 전자상거래 기업의 경우 특히 유의하여야 할 사항은, 정보통신서비스 제공자에게 적용되는 특례규정에 따라서, 위탁자가 관리/감독 또는 교육을 소홀히 하여 수탁자가 개인정보법의 규정을 위반한 경우 관련 매출액의 3%까지 과징금이 부과될 수 있다는 점이다(개인정보법 제39조의15 제1항 제4호). 현실적으로 수탁사의 업무처리를 감독하는 것이 쉽지는 않은 상황에서 이와 같은 과징금은 상당한 부담이 될 수 있다.

23)
본건은 유통회사가 가지고 있는 패밀리카드 회원들의 성명 · 주민등록번호 · 연락처 등 개인정보를 보험회사들이 사전에 마케팅을 위한 퍼미션 컬을 하기 이전에 소위 '필터링'을 한 사안이다. 즉, 보험회사들은 패밀리카드 회원 중 보험회사의 보험가입자나 블랙리스트에 올라 있는 사람 등을 걸러냄으로써, 즉 보험상품 판매에 적합한 대상자를 선정함으로써 보험 텔레마케팅의 효율을 높이기 위하여 필터링을 하였고, 이후 필터링에 기반하여 유통회사가 텔레마케팅을 한 사안이다. 본 사안에서 유통회사와 보험회사들은 이와 같은 필터링 작업을 위하여 유통회사의 회원들의 개인정보를 보험회사에게 제공한 것은 '위탁'이라고 주장하였다. 대법원은 이에 대하여 본 필터링은 보험 텔레마케팅 업무를 분담 · 지원하는 성격을 가지므로, 설령 사전필터링을 퍼미션 콜 업무의 부수업무로 보더라도 유통회사의 업무임과 동시에 위 보험회사들의 업무로서의 성격을 가지고, 위 보험회사들은 위와 같은 업무 처리에 관하여 독자적인 이익을 가진다고 볼 수 있다고 판시하였다.

24)
공개대상은 위탁업무의 목적 및 범위, 재위탁 제한에 관한 사항, 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항, 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항, 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항, 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항, 개인정보의 기술적·관리적 보호조치에 관한 사항 등이다.

25)
다만, 인터넷 홈페이지를 운영하지 아니하는 위탁자의 경우에는 사업장 등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.

4. 가명정보와 익명정보

GDPR상의 개념인 가명정보와 익명정보의 개념을 도입한 것은, 이번 데이터 3법 개정의 가장 중요한 특징이라 할 수 있다. 전자상거래 기업이 가지고 있는 개인정보에는 일반적인 의미에서의 개인정보 이외에도 개인신용정보가 포함되어 있다. 개인신용정보의 가명화에 관하여는 신용정보법이 적용되므로 신용정보법에 따른 절차를 밟아야 한다.

익명정보는 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보로서, 익명처리된 정보는 더 이상 정보주체를 식별할 수 없는 정보이므로 그 이용에 있어서 개인정보법이나 신용정보법의 각종 규제를 적용받지 않는 것이 원칙이다(개인정보법 제58조의 2).

가명정보란 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보를 말한다.[26] 가명정보는 통계작성, 과학적 연구 및 공익적 기록보존 등을 위하여 정보주체의 동의 없이도 처리할 수 있다(개인정보법 제28조의2 제1항). 개인정보법상 '처리'라고 함은 개인정보의 수집, 생성, 저장, 가공, 이용, 제공 공개, 파기 등의 제반 행위를 의미한다(동법 제2조 제2호). 따라서 가명정보에 해당한다면, 위의 3가지 목적으로는 정보주체의 동의가 없다고 하더라도 수집하고 스스로 이용하는 것 이외에 제3자 제공까지 할 수 있다. 다만 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보는 포함되어서는 안된다(동법 제28조의2 제2항).

가장 논란이 많았던 부분 중 하나는 통계작성과 과학적 연구의 범위를 어떻게 해석할 것인가 하는 것이다. 개인정보법은 통계작성과 과학적 연구라고 규정하면서(개인정보법 제28조의2 제1항), '과학적 연구'란 기술의 개발과 실증, 기초 연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구라고 정의하고 있다(동법 제2조 제8호). 반면 신용정보법은 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우에는 개인신용정보 제공·활용에 대한 동의가 필요 없는 것으로 규정하면서, '통계작성'에는 시장조사 등 상업적 목적의 통계작성을 포함하며, '연구'에는 산업적 연구를 포함하는 것으로 규정하고 있다(신용정보법 제32조 제5항 제9의2호).

여기에서 개인정보법상의 '통계작성'이 상업적 목적을 위한 경우까지 모두 포함하는 것인지 여부와 관련하여, 기본적으로 통계작성의 목적에 대하여 특별한 제한을 두고 있지 않으므로 상업적 목적의 통계작성도 포함된다고 해석된다.[27] 유사한 규정을 두고 있는 신용정보법에서는 통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함한다고 명시적으로 규정하고 있다(동법 제32조 9의2호).

한편, 가명정보의 제공 자체는 통계작성 목적으로 이루어졌는데, 이후 제공받은 자가 통계작성 목적 이외에도 과학적 연구, 공익적 기록 보존 목적으로는

26) "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다(개인정보법 제2조 제1호 및 1호의 2). 가명정보 및 처리의 개념 자체는 신용정보법도 유사하다(신용정보법 제2조 15호 및 16호).

27) 개인정보보호위원회, 같은 책, 제221면도 같은 견해이다.

동의 없이 '처리' 할 수 있는 것으로 해석하는 견해가 유력하다.[28] 일반 개인정보와는 달리 제공받은 목적 범위 내에서 사용하여야 한다는 제한 규정이 없기 때문이다(물론 통계작성, 과학적 연구, 공익적 기록 보존 목적 중 하나로만 사용할 수 있다). 한편, 가명정보를 과학적 연구 등 법에서 허용하는 범위로 제공하면서 대가를 받는 것은 금지하고 있지 않지만, 과학적 연구 등으로 처리하려는 사람에게 판매하려는 경우 등 판매 자체가 목적인 경우에는 허용되지 않는 것으로 보는 견해가 있다.[29]

이와 같이 가명정보처리에 대하여 융통성을 열어준 것은 '데이터 경제' 및 이에 바탕을 둔 4차 산업혁명의 바탕을 마련하고자 하는 입법적·정책적 고려의 일환이라고 할 수 있다. 전자상거래 기업들로서는 기존에 자신들이 보유한 데이터를 스스로 혹은 제3자의 데이터와 결합하여 활용할 수 있는 단초를 마련한 것이다. 다만, 가명정보라고 하더라도 다른 데이터와 결합하게 되면, 그 식별가능성이 높아질 수 있다. 특히 인공지능과 같이 데이터 분석기술이 고도화되면 더욱 그와 같은 위험성은 높아진다고 할 수 있다. 이와 같은 위험성에 대비하여 가명정보의 결합 및 재식별 금지에 대한 여러 가지 제한을 두고 있다.

즉, 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행할 수 있다. 또한 그 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 익명정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다. 「가명정보 결합 및 반출 등에 관한 고시」("결합고시")[30]가 이에 관한 상세한 규정을 두고 있다. 다만, 가명정보결합에 관한 상세한 내용은 본고의 범위를 넘는 것이어서 생략하기로 한다. 개인정보법상 가명정보결합에 있어서 특이한 점은 한국인터넷진흥원을 결합키 관리기관으로 별도로 인정하고 있다는 점이다. 즉, 가명정보의 결합을 원하는 기업은 결합전문기관에 결합 신청을 하게 되지만, 결합에 있어서 핵심적인 역할을 하는 결합키[31]는 결합키 관리기관인 한국인터넷진흥원에게 송부하고, 그 외의 결합을 하려는 정보는 결합전문기관에게 송부하여야 한다. 이후 결합키 관리기관은 결합신청자로부터 결합키를 제공받아 지체없이 결합키 연계정보를 생성하여 결합전문기관에 제공하여야 한다. 한편 결합전문기관은 결합키 관리기관으로부터 결합키 연계정보를 제공받아 가명정보의 결합을 완료하는 등으로 결합키 연계정보가 불필요하게 된 때에는 이를 지체없이 파기하여야 한다(결합고시 제9조).

한편 신용정보법의 경우, 가명정보의 결합은 데이터전문기관을 통하여 결합을 하도록 하면서, 개인정보법과는 달리 결합키전문기관을 따로 지정하지 않는다. 즉 결합키연계정보를 생성하는 별도의 기관이 없으며, 결합의뢰기관이 직접 결합키를 생성하되 그 생성방식은 공개하지 못하도록 하고 있다(신용정보법 제17조의 2, 제26조의 4, 신용정보업 감독규정 제15조의2).

참고로 신용정보법에 따른 가명정보 결합 규율대상에서 일반 상거래 기업 및 법인(신용정보법 제45조의3에 따른 상거래기업 및 법인)은 제외된다(신용정보

28) 개인정보보호위원회, 같은 책, 제224면도 같은 견해이다.

29) 개인정보보호위원회, 같은 책, 제224면

30) 2020. 8. 26. 개인정보보호위원회 의결

31) 이때 "결합키"란 결합 대상인 가명정보의 일부로서 해당 정보만으로는 특정 개인을 알아 볼 수 없으나 다른 정보주체와 구별할 수 있도록 조치한 정보를 말한다(결합고시 제2조 제3호). 또한 "결합키연계정보"란 동일 정보주체에 관한 가명정보를 결합할 수 있도록 서로 다른 결합신청자의 결합키를 연계한 정보를 말한다(동조 제4호).

법 제17조의2 제1항, 신용정보법 시행령 제14조의2 제1항). 또한 신용정보법에 따른 결합 관련 규정은 결합의뢰기관이 데이터전문기관 중 개인정보법에 따른 전문기관으로도 지정된 기관에서 개인정보법에 따른 결합 절차와 방법, 반출 및 승인 기준·절차 등에 따라 정보집합물을 결합하려는 경우에는 적용하지 않는다(신용정보법 시행령 제14조의2 제8항).

앞서 본 바와 같이 민간 기업들도 관련 요건을 갖추면 데이터결합전문기관으로 지정을 받을 수 있다. 이에 대하여 해당 민간 기업이 가지고 있는 데이터와 다른 신청기관의 데이터를 결합하는 것이 가능한지(소위 "셀프결합")에 관하여는, 데이터 활용의 효율성과 이해관계의 충돌이라는 관점에서 논란이 있다. 이에 관하여 보호위원회와 금융감독당국은 이에 대하여 원칙적으로 부정적인 입장을 보이고 있다.[32)33)]

가명정보는 재식별위험성이 있을 수 있으므로, 개인정보처리자는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다(개인정보법 제28조의4 제1항). 한편, 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다(동조 제2항).

32) 이데일리, 2020. 8. 26, [일문일답]개보위 "결합전문기관 9월 중 지정 목표…셀프결합 허용 안해"

33) 금융위원회, 금융분야 가명처리·익명처리 안내서(안), 2020. 7, 제70면

5. 보관 / 파기 및 기타 정보보호의무

전자상거래 기업들은 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 복구 또는 재생되지 않는 방법으로 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다(개인정보법 제21조 제1항 및 제2항, 동법 시행령 제16조).

전자상거래 기업들은 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다(개인정보법 제29조, 동법 시행령 제30조).

또한 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다. 이때 개인정보처리자는 사업주 또는 대표자 혹은 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)으로 지정하여야 한다(동법 제31조, 동법 시행령 제32조 제2항).

IV. 전자상거래에 있어서 개인정보 관련 몇 가지 쟁점

1. 전자금융거래와 개인(신용)정보

전자상거래 기업은 기본적으로 비대면으로 거래를 하게 되고, 그 과정에서 대금은 전자적 방법으로 지급결제가 이루어지게 된다. 그 과정에서 주로 신용카드가 가장 많이 사용되고, 이외에도 직불형 및 선불형 지급 수단이 병행적으로 사용되고, 결제 과정에서 지급수단 발행인(예: 신용카드 발행회사), PG사[34], VAN[35]사가 주로 참여하게 된다. 이와 같은 전자금융거래에 대하여는 전자금융거래법과 여신전문금융업법이 주로 적용된다. 본고에서는 전자금융과 관련한 금융규제 측면보다는 개인정보 관점에서 살펴보고자 한다.

34) PG란 Payment Gateway의 약어로서, 지급결제 대행업체를 의미한다.

35) VAN 사업자는 부가통신사업자, 즉 Value Added Network 사업자의 약어이다.

신용카드업자(전업카드사와 은행 등 겸영카드사)들이 개별적으로 다수의 판매자들을 관리하는 것이 사실상 불가능하기 때문에 이를 중간에서 중개하여 주는 VAN 사업자와의 계약을 통하여 지급결제정보를 송수신하게 된다. 한편, 전자상거래 기업들 전부가 실제로 전자결제에 필요한 인적·물적 설비를 다 갖추는 것이 어렵기 때문에, 이들을 대리하여 신용카드사의 가맹점 역할을 해주는 사업자를 PG라고 하고, 실제 판매자들은 PG의 하위 가맹점이 된다.[36]

36) 예자선, 핀테크 규제와 실무, 삼일인포마인, 2020, 제44-45면, 제50면

전자상거래 기업이 직불형 혹은 선불형 지급수단을 통하여 직접 대금을 결제하는 경우에는 해당 전자상거래 데이터는 전자상거래 기업에 모이게 된다. 그러나 전자상거래 기업이 신용카드를 통하여 결제를 받는 경우, 신용카드사는 물론이고 특히 PG / VAN사의 관여가 일정한 정도로 있게 되고, 해당 전자상거래 관련 데이터는 PG / VAN사에도 쌓이게 된다. 이와 같은 데이터(특히 개인정보)를 어떻게 관리하고 활용할 수 있을지가 현대 전자상거래에 있어서는 매우 중요한 쟁점이라고 할 수 있다.

신용카드 사용자들은 신용카드 발급신청을 하면서 개인(신용)정보를 신용카드사가 수집하고 일정한 목적으로 활용하는 것에 동의하였으므로, 신용카드사가 해당 정보를 수집하고 활용하는 것은 그 동의 범위 내에서는 가능하다고 할 것이고, 가명·익명 정보로 활용하는 것 역시 법령에 따라서 활용하는 것은 가능하다고 할 것이다.

PG사의 경우 지급수단 발행인과 가맹점 사이에서 결제정보 처리와 자금정산 업무를 지원하면서 정산 대금까지 직접 취급하므로 독립적인 전자금융업무의 주체이다. PG사의 경우 독립적으로 개인(신용)정보 수집·이용·제공에 관한 동의를 받았다면 PG사의 고유의 이익을 위하여 사용할 수 있다.

VAN사의 경우 정산대금은 취급하지 않는 업무위수탁 관계에 해당하고, 별도의 개인(신용)정보의 제3자 제공 동의는 필요로 하지 않는다.[37] 따라서 VAN사의 경우는 개인정보법 및 신용정보법의 관점에서 보면 수탁자로서의 역할을 하면서 그 업무 수행과정에서 개인(신용)정보를 보유하게 된 것이므로, VAN사

37) 예자선, 같은 책, 제62면

는 해당 정보를 그 고유의 이익을 위하여는 사용할 수 없다. 이는 개인정보 위·수탁의 가장 기본적인 원칙에 따른 것이다.

한편, 해당 VAN사들이 보유한 개인(신용)정보를 가명처리 내지 익명처리를 하여 사용할 수 있는지 여부는 좀더 논의가 필요할 것으로 보인다. 우선 VAN사들은 신용카드사 및 가맹점들과 서비스 제공에 관한 기본 약정을 체결하게 된다. 해당 약정에 의하면 PG / VAN사들은 그 업무수행과정에서 취득한 정보들을 임의로 활용하지 못하도록 하는 규정이 있는 경우가 있다. 이 조항을 엄격하게 해석하면 해당 정보들을 가명화 내지 익명화하여 활용하는 것도 해당 조항을 위반한 것으로 볼 여지가 있다. 한편, 개인정보 "처리"의 개념에 가명·익명 처리를 포함하는 것으로 해석한다면, VAN사는 수탁사로서 그 고유의 이익을 위하여 개인(신용)정보를 "처리"할 수 없으므로 가명·익명처리도 할 수 없다는 의견도 있다. 결국 이 부분은 VAN사와 신용카드사 및 가맹점 사이의 약정에 보다 명확하게 규정되는 것이 필요할 것이다.

2. 마이데이터 / 개인신용정보 전송요구권과 전자상거래

신용정보법의 개정으로 본인신용정보관리업("마이데이터")의 개념이 도입되었다. 이 과정에서 전자상거래를 통하여 축적된 정보 역시 관련 규정에 의하여 마이데이터 사업자에게 전송하여야 하는 상황도 예상이 된다.

마이데이터 사업이라 함은 개인인 신용정보주체의 신용관리를 지원하기 위하여 신용정보를 통합하여 그 신용정보주체에게 제공하는 행위를 영업으로 하는 것을 의미한다(신용정보법 제2조 제9의2호). 마이데이터 사업자는 신용정보의 통합제공이라는 고유업무 이외에도 관련 규정에 의하여 전송받은 데이터를 활용하는 여러 가지 사업을 할 수 있다(그 내용에 따라 이를 겸영업무 내지 부수업무라고 한다). 겸영업무의 대표적인 것은 투자자문업 또는 투자일임업이 있고(신용정보법 제11조 제6항), 부수업무의 대표적인 것은 데이터분석 및 컨설팅, 개인신용정보 관리계좌 제공 등의 업무가 있다(신용정보법 제11조의2 제6항).

신용정보법에 따라서, 정보주체는 신용정보제공·이용자등에 대하여 마이데이터 사업자(본인신용정보관리회사) 및 다른 금융기관에 대하여 본인에 관한 신용정보를 제공하여 줄 것을 요청할 수 있다(신용정보법 제33조의2 제1항). 그 전송요구 대상 정보의 범위는 신용정보제공 · 이용자등(전자상거래기업 포함)이 신용정보주체로부터 수집하거나 신용정보주체가 제공한 정보, 신용정보주체와 신용정보제공·이용자등 간의 권리·의무 관계에서 생성된 정보를 대상으로 한다. 다만 그 신용정보는 컴퓨터 등 정보처리장치로 처리된 신용정보일 것을 요구하고, 신용정보제공·이용자등이 개인신용정보를 기초로 별도로 생성하거나 가공한 신용정보는 이에 포함되지 아니한다(동조 제2항). 이와 같은 전송요구를 받은 신용정보제공·이용자등은 지체 없이 본인에 관한 개인신용정보를 컴퓨터 등 정보처리장치로 처리가 가능한 형태로 전송하여야 한다(동조 제3항).

한편, 동법 시행령 제28조의 3 제6항에서는 전송요구권의 대상인 신용정보의 범위를 보다 구체적으로 정의하고 있다. 즉, 동 조항에 따르면 동법 제2조 제9호의2의 각 목에 따른 정보를 포함하고 있고, 동법 시행령 제2조 제22항 및 제23항에 따른 동 시행령 별표 1 '신용정보관리업에 관한 신용정보의 범위'에 의하면 카드 정보에서는 카드 고객 정보와 카드 이용정보를 포함하고 있고, 전자지급수단 관련 정보에는 주문내역도 모두 포함하도록 되어 있다. 또한 동 조항에는 전기통신사업법 제6조에 따른 기간통신사업자에 대한 통신료 납부정보, 소액결제 정보 및 이와 유사한 정보로서 신용정보주체의 거래내역을 확인할 수 있는 정보가 포함되어 있다. 참고로 신용정보의 범위에는 상법 제46조에 따른 상행위에 따른 상거래의 종류, 기간, 내용, 조건 등에 관한 정보가 포함되어 있다(신용정보법 제2조 제1호의 제3호 마.목). 따라서 이상의 내용들을 종합하면, 전자상거래 기업도 상거래에 관한 광범위한 내용의 정보 등을 마이데이터 사업자에게 이전하여야 하는 것으로 해석될 수 있다.

이에 대하여는 특히 전자상거래 기업들로부터 강한 반발이 있다. 2020. 8. 19. 한국인터넷기업협회와 한국온라인쇼핑협회는 주문내역 정보는 신용정보가 아니라고 주장하면서 시행령을 재개정하여야 한다고 주장한다. 한편 금융당국은 신용정보의 개념에 상법상 상행위에 따른 상거래의 종류·기간·내용·조건 등에 관한 정보도 포함되므로 전송요구권의 대상에 주문내역 정보가 포함된다고 해석하고 있다. 다만, 금융위도 이에 대한 산업계의 반발을 의식하여 현재 다각도로 산업계와 협의를 하고 있는 것으로 보인다.[38)]

3. 전자상거래 등에서의 소비자보호에 관한 법률

전자상거래에 기본적으로 적용되는「전자상거래 등에서의 소비자보호에 관한 법률」("전자상거래법")에서도 개인정보에 관한 조항이 포함되어 있다.

전자상거래법은 전자상거래 기업에 대하여 전자상거래 및 통신판매에서의 표시·광고, 계약내용 및 그 이행 등 거래에 관한 기록을 상당한 기간 보존하고, 소비자가 쉽게 거래기록을 열람·보존할 수 있는 방법을 제공하도록 의무를 부과하고 있다. 이때 사업자가 보존하여야 할 거래기록 및 그와 관련된 개인정보(성명·주소·전자우편주소 등 거래의 주체를 식별할 수 있는 정보로 한정한다)는 소비자가 개인정보의 이용에 관한 동의를 철회하는 경우에도 정보통신망법 등 대통령령으로 정하는 개인정보보호와 관련된 법률의 규정에도 불구하고 이를 보존할 수 있다(동법 제6조 제1항 및 제2항). 여기서 대통령으로 정하는 개인정보보호규정은 정보통신망법 제30조 제3항[39)], 개인정보법 제21조 제1항 본문[40)], 제36조 제2항[41)] 및 제37조 제4항[42)], 신용정보법 제37조 제1항 본문[43)]을 의미한다(동법 시행령 제5조).[44)]

한편, 전자상거래 기업들은 계약 또는 청약철회 등에 관한 기록 혹은 대금결제 및 재화등의 공급에 관한 기록은 5년간 보존하되, 소비자들에 대하여는 해당

38) 중앙일보, 2020. 8. 31. "'짜장면 1그릇 주문'은 신용정보일까? 마이데이터 정보제공 논쟁"

39) 정보통신서비스 제공자등은 이용자가 동의를 철회하면 지체없이 수집된 개인정보를 복구/재생할 수 없도록 파기하는 등의 조치를 취하여야 한다. 동 조항은 개인정보법 제39조의 7(이용자의 권리 등에 대한 특례) 제3항으로 이동하였고 내용은 같다.

40) 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 동 조항은 변경되지 아니하였다.

41) 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다. 동 조항은 변경되지 아니하였다.

42) 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다. 동 조항은 변경되지 아니하였다.

43) 개인인 신용정보주체는 제32조제1항 각 호의 방식으로 동의를 받은 신용정보제공·이용자에게 개인신용평가회사, 개인사업자신용평가회사 또는 신용정보집중기관에 제공하여 개인의 신용도 등을 평가하기 위한 목적 외의 목적으로 행한 개인신용정보 제공 동의를 대통령령으로 정하는 바에 따라 철회할 수 있다. [변경 전 조항: 개인인 신용정보주체는 제32조제1항 각 호의 방식으로 동의를 받은 신용정보제공·이용자에게 신용조회회사 또는 신용정보집중기관에 제공하여 개인의 신용도 등을 평가하기 위한 목적 외의 목적으로 행한 개인신용정보 제공 동의를 대통령령으로 정하는 바에 따라 철회할 수 있다.]

44) 다만 이번 데이터 3법 개정에 따라 위 조항은 그 위치에 변동이 있으므로, 전자상거래법 및 동법 시행령도 이와 연동하여 개정될 필요가 있다.

사이버몰에서 거래기록을 열람하고 이를 전자문서의 형태로 저장할 수 있도록 하여야 한다. 만일 소비자가 원한다면 그 거래기록을 방문, 전화, 팩스 또는 전자우편의 형태로 열람하거나 복사할 수 있도록 하여야 한다. 특히 개인정보의 이용에 관한 동의를 철회한 소비자의 거래기록 및 개인정보를 보존하는 경우에는 이용에 관한 동의를 철회하지 아니한 소비자의 거래기록 및 개인정보와 별도로 보존하도록 규정하고 있다(동법 시행령 제6조). 다만 소비자가 사업자의 사업활동을 방해할 목적으로 계속하여 반복적으로 요구하는 경우에는 그 열람에 응하지 않을 수 있다(전자상거래 등에서의 소비자보호 지침 제4조).

이와 같이 전자상거래 기업들에 대하여 소비자(정보주체)의 개인정보처리에 관한 동의의 철회에도 불구하고 해당 기록을 보관하도록 하는 이유는, 거래기록의 보존을 통하여 거래의 안정성을 확보하려는 것이다. 이는 여러 가지 익명의 전자상거래에 따른 부작용을 최소화하고, 경우에 따라 특정 소비자(소위 블랙컨슈머)가 자신의 개인정보처리에 관한 동의를 철회한 후 해당 거래에 관한 이의를 제기하게 되는 경우에 대응할 수 있도록 하는 것이다.

또한 전자상거래법은, 전자상거래 기업이 판매 목적으로 소비자에 관한 정보를 수집하거나 이용(제3자 제공 포함)할 때에는 정보통신망법 등 관계 규정에 따라 이를 공정하게 수집하거나 이용하여야 하고, 만일 거래에 있어서 소비자에 관한 정보가 도용되어 소비자에게 손해발생 혹은 그와 같은 우려가 있는 특별한 사유가 있는 경우에는 본인확인 및 해당 소비자에 대한 관련 거래 기록의 제공, 도용에 의하여 변조된 소비자에 관한 정보의 원상회복, 도용에 의한 피해의 회복 등 필요한 조치를 하도록 하고 있다(동법 제11조 및 동법 시행령 제12조). 가령 소비자에게 3개월 무료 이용 등의 이익 제공을 약속하면서 소비자에 관한 정보를 수집한 후 실제로 약속을 이행하지 않는 행위는 공정하게 수집하는 방법으로 볼 수 없다(전자상거래 등에서의 소비자보호 지침 제7조 가항).

한편, 사업자는 소비자 본인의 요청에 의하여 도용 여부 확인 및 관련 거래 기록의 제공을 위하여 (1) 본인확인 방법으로 휴대폰 인증, 공인인증서 등의 방법 중 2가지 이상을 갖추고 소비자가 선택한 방법에 의하여 본인확인 절차를 거쳐야 하고, (2) 소비자가 본인에 대한 거래 기록을 요청하는 경우 본인확인 절차를 거친 후 제공하여야 하며, (3) 소비자가 도용을 신고한 경우 신고접수 직원의 성명을 알려주는 등 신고접수 및 처리상황을 쉽게 확인할 수 있는 방법을 소비자에게 알려주어야 한다(동 지침 제7조 나항). 또한 소비자의 소비자의 계정(ID), 비밀번호, 신용카드번호 등이 도용된 경우 즉시 원상회복에 관한 조치를 취하여야 한다(동 지침 제7조 다항).

이상의 규정들은 전자상거래에 있어서는 소비자의 정보가 불공정하게 수집되거나 도용될 가능성이 상대적으로 높기 때문에, 사업자들에 대하여 즉각적인 보호조치를 취하도록 요구하고 있는 것이다.

4. 맞춤형 광고와 행태정보의 수집

전자상거래의 경우 그 구매이력 내지 구매를 위하여 다른 상품을 살펴본 내역들이 오프라인에서의 거래보다 더 상세하게 저장되기 때문에 사업자들은 그 구매정보를 분석하여 개별적인 맞춤형 광고를 통하여 그 매출을 확대하려는 노력을 하게 된다. 이와 같은 구매이력 내지 검색이력과 같은 행태정보 역시 개인의 프라이버시와 깊은 관련이 있으므로 이와 같은 맞춤형 광고 및 이를 위한 행태정보의 수집에 대하여도 개인정보법, 정보통신망법 이외에「위치정보의 보호 및 이용 등에 관한 법률」("위치정보법")이 적용될 수 있다. [45)]

45) 안정민, 최경진, "맞춤형 광고와 개인정보보호," 미국헌법연구 제28권 제3호(2017), 129-135면

행태정보 역시 개인정보에 해당할 수 있으며 이 경우 전자상거래 기업들은 개인정보법 소정의 정보통신서비스 제공자에 대한 특례 규정을 우선적으로 적용받게 된다. 따라서 그와 같은 정보를 수집하려면 우선적으로 소비자의 동의가 전제되어야 한다(동법 제39조의 3 제1항). 서비스 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적 · 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란하거나 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우에는 동의를 받지 않을 수도 있으나, 맞춤형 광고를 위한 행태정보의 수집이 이에 해당한다고 보기는 어렵다.

결국 전자상거래 기업들이 수집하는 정보가 개인정보에 해당하는 한, 그의 수집 및 자체 분석은 소비자의 동의를 기반으로 하는 것이 원칙이라고 할 수 있다. 실무적으로 상당 수의 기업들이 사용하는 구글 애널리틱스의 경우, 웹사이트 트래픽과 관련한 여러 가지 정보를 기업들이 수집하여 구글에 제공하게 된다. 이때 상당히 많은 정보가 제공되는데, 명확하게 개인정보라고 할 수 있는 정보라고 할 수 없는 것들이 대다수이고, 일부 개인을 식별할 수 있는 가능성이 있는 정보들은 비식별화 조치[46)]를 통하여 개인정보의 제3자 제공이 되지 않도록 하는 경우가 일반적이다.

46) 여기서 비식별화 조치라 함은 일반적인 의미에서 최대한 개인의 식별가능성을 없애는 방법으로 조치를 한 것을 의미한다.

(1) 온라인 맞춤형 광고 가이드라인

방송통신위원회는 2017. 2. 온라인 맞춤형 광고 개인정보보호 가이드라인("맞춤형 광고 가이드라인")을 발표하여 이와 관련한 내용을 좀더 상세하게 규율하고 있다. [47)]

47) 동 가이드라인 I.에 의하면 2019. 9. 1.을 기준으로 매 3년이 되는 시점마다 그 타당성을 검토하여 개선 등의 조치를 취하도록 하고 있다.

동 가이드라인의 적용대상인 온라인 행태정보라 함은 웹 사이트 방문 이력, 앱 사용 이력, 구매 및 검색 이력 등 이용자의 관심, 흥미, 기호 및 성향 등을 파악하고 분석할 수 있는 온라인상의 이용자 활동정보를 의미한다. 이와 같은 행태정보를 처리하여 이용자의 관심, 흥미, 기호 및 성향 등을 분석·추정한 후 이용자에게 맞춤형으로 제공되는 온라인 광고를 온라인 맞춤형 광고라고 한다. 이와 같은 행태정보를 자사 또는 타사의 웹사이트 및 앱 등 온라인 매체를 통해 수집하고 온라인 맞춤형 광고를 전송하는 "광고" 사업자[48)]가 있고, 자사 웹사이트 및 앱 등 온라인 매체를 통해 행태정보의 수집을 허용하거나 온라인 맞춤형 광고가 전

48) 당사자 광고사업자와 제3자 광고사업자로 나눌 수 있다.

송되도록 하는 "매체" 사업자[49]가 존재한다.

자사 웹사이트나 앱을 통하여 맞춤형 광고를 직접 전송하는 광고 사업자는 이용자가 언제든지 쉽게 확인할 수 있도록 웹사이트나 앱에 수집하는 행태정보의 항목, 수집 방법, 목적, 보유·이용 기간, 이용자 통제권 및 피해구제 방법을, 홈페이지의 첫 화면 또는 광고가 제공되는 화면 등을 통하여 상세히 안내하여야 한다. 한편, 다른 사업자가 운영하는 웹사이트나 앱을 통하여 맞춤형 광고를 전송하는 광고 사업자는 온라인 맞춤형 광고 내부나 주변부에 이용자가 쉽게 식별할 수 있는 표지(標識)를 설치하고, 표지와 링크된 별도 페이지에 행태정보를 수집·처리하는 사업자명과 앞서 본 행태정보 관련 기본적인 내용을 상세히 안내하여야 한다. 이 때, '안내 표지(, 등)'가 '광고'와 충분히 구분될 수 있게 화면을 구성하여, 이용자가 '안내 표지'를 클릭하였음에도 '광고'가 클릭되지 않도록 조치해야 한다. 한편 매체 사업자가 자사 웹사이트 및 앱을 통하여 광고 사업자가 이용자의 행태정보를 수집할 수 있도록 허용한 경우, ① 행태정보를 수집·처리하는 광고 사업자명, ② 행태정보 수집 방법 등을 이용자가 쉽게 알 수 있도록 홈페이지의 첫 화면 또는 광고가 제공되는 화면 등을 통해 표시하여야 한다.

광고 사업자는 사상, 신념, 가족 및 친인척관계, 학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 민감한 행태정보를 수집하지 않도록 노력하여야 하며, 이용자의 동의 없이는 행태정보를 이용·분석하여 민감정보를 수집·생성·활용하여서는 아니된다. 또한 광고 사업자는 만 14세 미만임을 알고 있는 아동이나 만 14세 미만의 아동을 주 이용자로 하는 온라인 서비스로부터 맞춤형 광고 목적의 행태정보를 수집하지 않아야 하며, 만 14세 미만임을 알고 있는 아동에게 맞춤형 광고를 제공하여서는 아니된다.

광고 사업자 또는 매체 사업자가 직접 수집한 행태정보를 제3의 광고 사업자에게 제공하는 경우, ① 행태정보를 제공받는 자, ② 제공하는 행태정보의 항목 및 ③ 행태정보를 제공받는 자의 이용 목적 등을 이용자가 쉽게 알 수 있도록 홈페이지의 첫 화면 또는 광고가 제공되는 화면 등을 통해 표시하여야 한다.

만일 광고 사업자가 행태정보와 개인 식별정보를 결합할 경우에는 이용자에게 해당 사실과 사용목적, 결합되는 정보항목, 보유기간 등을 명확히 알리고, 해당 이용자로부터 사전에 동의를 받아야 한다.

동 가이드라인의 입장은 행태정보의 수집의 경우, 개인 식별정보와 결합하기 이전까지는 개인정보로 보지 않으므로 행태정보 수집 자체에 대하여 소비자의 동의를 요구하지는 않으면서도, 행태정보를 수집한다는 사실 자체 및 관련 내용을 소비자에게 미리 알리도록 함으로써, 소비자의 권리와의 균형을 맞추려고 하고 있는 것으로 보인다.

동 가이드라인은 이외에도 보다 적극적인 소비자의 통제권을 보장하고 있다. 즉, 광고 사업자는 이용자가 행태정보의 제공 및 온라인 맞춤형 광고 수신 여부를 쉽게 선택할 수 있도록 이용자가 광고화면을 통하여 직접 통제하도록 하거나

49) 포털사, 온라인 쇼핑몰, 온라인 게임회사, 온라인 미디어 등

이용자가 컴퓨터나 스마트폰 등의 단말기에서 쿠키 및 인터넷 이용기록을 삭제·차단함으로써 맞춤형 광고를 통제할 수 있도록 하는 방법을 안내할 것을 요구하고 있다. 특히 광고 플랫폼 등을 이용하여 다른 사업자가 운영하는 웹사이트나 앱을 통하여 맞춤형 광고를 전송하는 광고 사업자의 경우 광고화면을 통하여 직접 통제하도록 하는 수단을 반드시 포함하여야 한다.

이와 같은 행태정보는 앞서 본 바와 같이 프라이버시 침해가능성이 높으므로, 광고 사업자는 행태정보의 유·노출, 부정사용 등을 방지하기 위해 개인정보법 소정의 기술적, 관리적 및 물리적 보호조치를 취하여야 한다. 또한 광고 사업자는 수집한 행태정보를 필요 최소한의 기간 동안만 저장하고, 목적 달성 후 즉시 파기하거나 안전한 분리저장 등의 조치를 취하여야 한다(광고 사업자는 행태정보 보유기간 및 목적을 명확히 안내하여야 한다. 특히, 보유기간은 이용자가 쉽게 이해할 수 있는 정확한 기간을 명시하여야 한다).

(2) 위치정보

한편, 행태정보의 수집 및 맞춤형 광고에 있어서 최근 개인의 위치정보가 매우 중요한 역할을 담당하게 되었다. 가령 특정 소비자가 특정 상점 위치에 가까이 갔을 때 해당 상점이 제공하는 각종 할인행사 신상품 소개 등의 정보를 보낼 수 있기 때문이다. 개인위치정보라 함은 특정 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 전시통신설비를 이용하여 수집된 것을 의미한다(위치정보법 제2조 제1호 및 제2호). 이와 같은 위치정보를 이용하는 사업에는 위치정보를 수집하여 위치기반서비스사업자에게 제공하는 위치정보사업자와 위치정보를 이용한 서비스를 제공하는 위치기반서비스사업자가 있다.

기본적으로 위치정보도 일반적인 개인정보처럼 정보주체의 동의가 있어야 이를 수집하고 이용·제공할 수 있다. 즉 위치정보사업자는 일정 사항을 이용약관에 명시한 후 정보주체의 동의를 받아야 위치정보를 수집할 수 있고(위치정보법 제18조), 위치정보를 이용하여 서비스를 제공하려는 위치기반서비스사업자 역시 일정 사항을 이용약관에 명시한 후 정보주체의 동의를 얻어야 한다(위치정보법 제19조). 이와 같은 동의를 얻은 위치기반서비스 사업자는 위치정보사업자에게 위치정보를 제공할 것을 요청할 수 있고, 위치정보사업자는 이를 정당한 사유가 없는 한 거절할 수 있다(위치정보법 제20조). 위치정보의 경우 실무적으로 중요한 것은, 다른 개인정보와는 달리 이를 수집하거나 이용하려면 개인위치정보를 대상으로 하는 위치정보사업자의 경우에는 방송통신위원회의 허가를 받아야 하고(위치정보법 제5조), 개인위치정보를 대상으로 하지 아니하는 위치정보사업자(사물위치정보사업자)와 개인위치정보를 대상으로 하는 위기반서비스사업자의 경우에는 (소상공인 등의 특례가 적용되는 경우를 제외하면) 방송통신위원회에 신고 하여야 한다(위치정보법 제5조의2, 제9조).

(3) 접근권한 통제

마지막으로 행태정보의 수집에 있어서의 가장 중요한 원천은 스마트폰 등의 단말기 내지 단말기의 이용을 도와주는 각종 애플리케이션("앱")이라고 할 수 있다. 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한("접근권한"이라 한다)이 필요한 경우, 해당 권한이 서비스 제공에 필수적이라면 접근권한이 필요한 정보 및 기능의 항목과 이유를 알리고 이용자의 동의를 받아야 한다. 만일 서비스 제공에 필수적이지 않다면, 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실도 함께 알려야 하고, 이용자가 동의하지 아니한다는 이유로 이용자에게 해당 서비스의 제공을 거부하여서는 아니 된다(정보통신망법 제22조의 2). 방송통신위원회는 이의 구체적인 실행을 위하여 스마트폰 앱 접근권한 개인정보보호 안내서를 2017. 3. 배포한 바 있다.

실무적으로는 해외의 사업자들이 자신들의 앱 개발을 마친 후 국내에서 앱을 출시하려고 하다가 이와 같은 내용을 반영하기 위하여 상당한 시간과 노력을 투자하는 경우를 많이 보아왔다. 우리나라의 규제와는 다른 환경에서 앱을 개발하는 과정에서 발생한 불가피한 경우인데, 국내 소비자들의 프라이버시를 위하여 필요한 면도 있다. 다만 위 규정의 취지를 반영하는 앱이라면 위의 가이드라인의 세부 내용과 일부 차이가 있더라도 불법이라고 보기는 어려울 것으로 생각한다.

5. 온라인 플랫폼 중개거래의 공정화에 관한 법률

2020. 9. 28. 공정거래위원회는「온라인 플랫폼 중개거래의 공정화에 관한 법률」("플랫폼 공정화법")을 입법예고하였다. 아직 입법예고 단계이고 향후 이에 관하여도 많은 논란이 있을 것으로 예상되므로, 실제 입법과정에서는 상당한 변경이 있을 수도 있지만, 전자상거래에 있어서 온라인 플랫폼이 차지하는 중요성은 그 어느 때보다도 높아졌으므로 이하에서는 간략하게 정부 발표안을 중심으로 논의를 하고자 한다.[50)]

기본적으로 본 플랫폼 공정화법의 입법의도는, 온라인 유통시장의 급성장 추세에 코로나19로 인한 비대면 거래의 폭발적 증가가 더해지면서 산업 전반에 걸쳐 온라인 플랫폼의 영향력이 급속히 확대됨에 따라 온라인 플랫폼에 대한 입점업체의 거래의존도가 급속히 높아지고 있는 상황에서, 온라인 플랫폼 사업자가 온라인 플랫폼 입점업체의 판매가격 또는 경영상대방 등 경영활동을 간섭하거나, 거래과정에서 발생한 손해를 입점업체에 일방적으로 전가하는 등의 불공정행위를 최소화하려는 것으로 보인다.

특히 온라인 플랫폼은 직접 거래에 참여하지 않는 중개사업자이므로, 자신의 명의로 소매업을 영위하는 사업자에게 적용되는「대규모유통업에서의 거래 공정화에 관한 법률」이 적용되지 않으며, 공정거래와 관련한 일반법인「독점규제 및 공정거래에 관한 법률」만으로는 그에 관한 특별한 상황에 대한 대응에는 한계가

50) https://www.moleg.go.kr/lawinfo/makingInfo.mo?lawSeq=60857&lawCd=0&&lawType=TYPE5&mid=a10104010000 (최종방문 2020. 11. 3.)

있기 때문에 온라인 플랫폼 중개거래에 관한 보다 상세한 규제를 하는 것이 입법 의도라고 할 수 있다.

동 법안에서 규정하는 "온라인 플랫폼"이란 둘 이상 집단의 이용자들 간에 재화 또는 용역의 거래, 정보 교환 등 상호작용을 목적으로 하는 인터넷 홈페이지, 모바일 응용프로그램 및 이에 준하는 전자적 시스템을 말한다. "온라인 플랫폼 중개서비스"란 온라인 플랫폼을 통하여 재화 또는 용역에 관한 정보제공, 소비자의 청약 접수 등 대통령령이 정하는 방식으로 온라인 플랫폼 이용사업자와 소비자 간 재화 등의 거래의 개시를 알선하는 서비스를 말한다. "온라인 플랫폼 중개거래"란 온라인 플랫폼 중개서비스업자가 온라인 플랫폼 이용사업자에게 온라인 플랫폼 중개서비스 등을 제공하고 그 대가로 수수료를 수취하는 거래를 말한다.

동 법의 적용범위는 온라인 플랫폼 중개서비스업자의 주된 사무소의 소재지 또는 설립 당시의 준거 법률에 관계 없이 국내 온라인 플랫폼 이용사업자와 국내 소비자 간 재화 등의 거래의 개시를 알선하는 온라인 플랫폼 중개서비스업자에 대하여 적용된다. 따라서 해외 사업자들도 국내 이용사업자와 소비자간에 거래 중개를 하는 경우에는 동 법의 적용을 받게 된다. 한편, 동 법은 일정한 규모 이상의 플랫폼에 대하여만 적용된다. 현재 안에 따르면, 직접 사업연도 매출액 100억원, 중개거래금액 1,000억원의 범위를 기준으로 적용될 것으로 예상된다(동법 제3조).

동 법안에서 주목할 만한 내용으로는 계약서 작성·교부 의무 및 필수기재사항 규정(안 제6조제1항·제2항)이 있다. 이로써 우월적 지위를 지닌 온라인 플랫폼 중개서비스업자에게 주요 거래조건 및 분쟁예방을 위한 사항을 계약서에 명시하도록 하고 이를 교부할 의무를 부여하고 있다. 또한 공정거래위원회는 표준계약서 제정·보급(안 제6조3항)도 염두에 두고 있는 것으로 보인다. 동 법안에 따르면 표준계약서에는 수수료, 계약기간 및 해지사유, 반품 등 절차 및 기준, 판매대금 정산 방식 및 시기, 다른 플랫폼 이용 제한 여부, 플랫폼사업자의 이용사업의 판매 방식 관련 제한, 할인쿠폰 발행 관련 사항, 판매과정에서 발생한 손해에 대한 분담 기준, 온라인 플랫폼 이용사업자가 판매하는 재화 등의 정보가 온라인 플랫폼에서 소비자에게 노출되는 방식 및 순서 결정 기준, 플랫폼 사업자가 직접 판매하는 상품과의 차별적 취급 여부 등에 관한 일반적인 내용 이외에도, 데이터 관점에서 온라인 플랫폼 이용사업자 및 소비자가 온라인 플랫폼을 이용하는 과정에서 생성된 정보를 온라인 플랫폼 이용사업자가 제공받을 수 있는지 여부, 제공 가능한 정보의 범위, 제공 방식 및 조건에 관한 내용이 포함되어 있다.

또한 온라인 플랫폼 중개사업자의 불공정거래행위 금지(안 제9조) 조항에 따라서, 부당하게 온라인 플랫폼 이용사업자가 구입할 의사가 없는 상품 또는 용역을 구입하도록 강제하는 행위 금지, 부당하게 온라인 플랫폼 이용사업자에게 거래과정에서 발생한 손해를 전가하는 행위 금지, 부당하게 온라인 플랫폼 이용사업자의 경영활동을 간섭하는 행위 금지와 같은 내용이 포함되어 있다.

공정거래위원회는 동법 위반사항에 대하여 시정명령(안 제25조)을 할 수 있

고, 필수기재사항을 기재한 계약서 서면교부 및 기명날인 의무, 불공정거래행위 금지를 위반한 온라인 플랫폼 중개서비스업자에게 대통령령으로 정하는 법 위반 금액의 2배를 초과하지 않는 범위 내에서 과징금을 부과할 수 있으며, 법위반 금액을 산정하기 곤란한 경우에는 10억원을 초과하지 않는 범위 내에서 과징금을 부과할 수 있도록 되어 있다(안 제29조). 해당 시정명령에 따르지 아니하면 2년 이하의 징역 또는 1억 5천만원 이하의 벌금에 처해질 수 있다(안 제33조).

IV. 맺음말

필자가 본고를 작성하면서 분량상의 제약에 비하여 다루어야 하는 쟁점들이 많아 그 깊이와 형식에 대한 고민이 있었다. 일단 데이터 3법 개정 후 2020. 8. 5.부터 시행되면서 아직은 실무상 많은 의문들이 있다는 점을 고려하여 특정 주제에 대하여 깊은 논의를 하기보다는, 전자상거래 기업들에 있어서 데이터 처리의 전반 및 각 단계별로 논의가 있는 부분을 짚어 보는 정도로 마무리하기로 하였다. 각 쟁점별로 더 심도 있는 논의는 별도의 기회로 미루기로 한다.