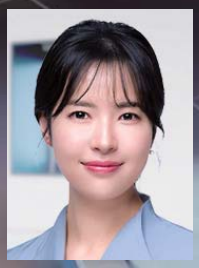
보험회사의 개인정보보호법 위반 과징금 관련 시사점과 대응방안



김소연
법무법인(유한) 세종 변호사

이창윤
법무법인(유한) 세종 변호사

Ⅰ•본건 제재의 개요

개인정보보호위원회(이하 '개보위')는 2024. 12. 11. 관련 보험사에 대한 조사(이하 '본건 조사') 결과를 바탕으로 제재를 의결하였다(이하 '본건 제재'). 위 의결의 요지는 (1) 적법한 동의 없이 개인정보를 수집해 마케팅에 활용한 보험사에 대해서는 과징금 총 92억 770만 원을 부과하고, (2) 개인정보 보호책임자(이하 'CPO')의 내부통제 역할도 강화하도록 시정명령하며, (3) 보험료 계산을 중단하거나 보험 계약을 체결하지 않은 이용자 정보를 파기하지 않고 1년간 보유하고 있는 것으로 확인된 보험사 모두에 대하여 보유기간을 개선하도록 시정명령하는 한편, (4) 1년이 경과하여도 이용자 정보를 파기하지 않은 보험사에는 과태료 540만 원을 부과하는 것이었다.

본건 제재 중 위 (3), (4) 부분, 즉 '처리 목적을 달성한 개인정보를 파기하지 않은 행위'에 관하여는 지면의 제약상 검토를 생략하고, 이하에서는 위 (1), (2) 부분, 즉 '적법한 동의 없이 개인정보를 수집하여 보험 마케팅(상품 소개)에 이용한 행위'에 관하여 주로 살펴보기로 한다.

개보위의 본건 제재 관련 보도자료에 따르면, 일부 보험사는 상품 소개를 위한 개인정보 처리에 명백히 미동의 의사를 표시한 이용자에게 동의의 변경을 유도하는 팝업창(이하 '재유도 창')을 운영하였는데, 이러한 재유도 창은 종전에 운영하던 재유도 창[1]의 '확인'과 '취소' 버튼의 효과를 변경하여, "상품 소개 항목에 동의하지 않을 경우 1:1상담 서비스 및 이벤트 안내 등 다양한 서비스를 제공받으실 수 없습니다. 상품소개에 동의 상태로 다음 단계를 진행하려면 〈확인〉 버튼을, 상품 소개에 동의하지 않고 진행하시려면 〈취소〉버튼을 클릭해주세요"[2]라는 문구에 대하여 '확인' 버튼을 누르는 경우 '동의'로 처리되면서 그 동의 내역이 변경된 것을 알 수 없도록 설계되어 있었다. 개보위는

1) 종전에는 '확인' 버튼을 누르는 경우 '미동의' 상태로 다음 절차로 넘어가고, '취소' 버튼을 누르면 재유도 창 이전 화면으로 돌아가서 정보주체가 직접 '상품 소개 항목에 동의'할 수 있도록 하였다.

2) H보험의 경우. 나머지 손해보험사의 경우에도 대체로 유사하나 세부 문구에 다소 차이가 있었다.

위와 같은 방식을 통하여 받은 동의는 오인할 수 있는 표현의 사용 및 개인정보 자기결정권의 제한에 의한 것이고, '개인정보 처리' 표현이나 동의에 필요한 법정 고지사항이 없었다는 점 등에서 적법하게 득한 동의가 아니라고 판단하였다. 한편 개보위는 위 재유도 창을 통해 이루어진 동의 절차는 마케팅 부서에서 기획한 것인데 그 과정에서 CPO의 검토 등 내부통제가 제대로 작동하지 않은 것이 확인되었다는 이유로 관련 보험사에 대해 CPO의 내부통제 절차가 적정하게 이루어지고 CPO가 독립적으로 역할을 수행할 수 있도록 시정명령하였다.

Ⅱ • 적용법률 및 처분청

「개인정보 보호법」(이하 '개인정보법') 제6조 제1항, 「신용정보의 이용 및 보호에 관한 법률」(이하 '신용정보법') 제3조의2에 따르면, 신용정보 중 개인의 신용도와 신용거래능력 등을 판단할 때 필요한 정보를 의미하는 '개인신용정보'에 관해서는 신용정보법이 개인정보법에 우선하여 적용되며, 신용정보법에 규정되지 않은 사항에 한하여 일반법인 개인정보법이 적용된다.

개인정보법이 적용될 경우에는 개보위가,[3] 신용정보법이 적용될 경우에는 금융위원회가,[4] 각 조사 또는 처분을 주관하는 주체가 된다. 신용정보법이 우선 적용되는 '개인신용정보'와 그렇지 않은 '그 밖의 개인정보'를 구분하는 기준은 '신용도 판단과 관련이 있는지 여부'가 될 것이고, 피조사자 등이 금융기관인 경우 (개인)신용정보 없이 순수한 개인정보만을 처리하는 경우가 많지 않아 대부분 신용정보법이 적용되고 금융위원회가 주관하는 것으로 이해되어 왔다.

그러나 본건 조사에서는 계약 체결 이전, 즉 마케팅 단계에 이루어진 개인정보 처리가 문제되어 개보위가 조사 및 처분을 주관하였고, 개보위는 본건 제재시 보도자료를 통하여 "비록 금융기관의 개인정보 처리라 하더라도 명백히 신용정보법상의 개인신용정보에 해당하지 않는 경우 개인정보 분야의 기본법인 개인정보법의 적용대상이 된다"라는 점을 강조하였다. 향후에도 개보위가 금융회사에 대해 보다 적극적으로 개인정보법을 적용해 나갈 것으로 예상되는 대목이다.[5]

---

3) 개인정보법 제7조의8 제3호
4) 신용정보법 제45조
5) 한편 개인정보법과 신용정보법은 과징금 산정 기준도 상이하게 규정되어 있어, 어떠한 법령이 적용되는지는 조사(검사) 대상자의 입장에서 중요한 의미가 있다. 이에 관해서는 별도 항목으로 후술한다.

Ⅲ • 적법한 동의 유무

개인정보법은 개인정보를 수집·이용하거나 제3자에게 제공하려 할 때 일정한 경우를 제외하고는 법정 고지사항을 알리고 정보주체의 동의를 받도록 하고 있고(제15조, 제17조)[6], 위 동의를 받지 아니하고 개인정보를 처리한 경우를 과징금 부과 대상으로 정하고 있다(제64조의2 제1항 제1호).

한편 대법원은, 구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2013. 3. 23. 법률 제11690호로 개정되기 전의 것. 이하 '정보통신망법')에 따른 정보통신서비스 제공자인 원고 회사가 오픈마켓 등 웹사이트의 배너 및 이벤트 광고 팝업창을 통하여 개인정보 수집 항목 및 목적, 보유기간에 대한 안내 없이 '확인'을 선택하면 동의한 것으로 간주하는 방법으로 명시적인 동의를 받지 않고 이용자 개인정보를 수집하여 보험사 등에 제공하였다는 이유로 방송통신위원회가 원고 회사에 시정조치 등을 한 사안에서, "정보통신서비스 제공자가 이용자로부터 개인정보 수집·제공에 관하여 정보통신망법에 따라 적법한 동의를 받기 위하여는, 이용자가 개인정보 제공에 관한 결정권을 충분히 자유롭게 행사할 수 있도록, 정보통신서비스 제공자가 미리 해당 인터넷 사이트에 통상의 이용자라면 용이하게 법정 고지사항의 구체적 내용을 알아볼 수 있을 정도로 법정 고지사항 전부를 명확하게 게재하여야 한다"라고 판시한 바 있다. 또한 "법정 고지사항을 게재하는 부분과 이용자의 동의 여부를 표시할 수 있는 부분을 밀접하게 배치하여 이용자가 법정 고지사항을 인지하여 확인할 수 있는 상태에서 개인정보의 수집·제공에 대한 동의 여부를 판단할 수 있어야 하고, 그에 따른 동의의 표시는 이용자가 개인정보의 수집·제공에 동의를 한다는 명확한 인식 하에 행하여질 수 있도록 그 실행방법이 마련되어야 한다"라고도 하였다(대법원 2016. 6. 28. 선고 2014두2638 판결).

본건 제재에서 개보위는 동의 과정 전반에서 이용자가 개인정보 처리에 관한 결정권을 충분히 자유롭게 행사할 수 있을 만큼의 환경이 제공되지 않았고, 따라서 적법한 동의 자체가 없이 개인정보를 수집·이용한 사안으로 판단한 것으로 보인다. 그러나 위 대법원 판례의 법리에 비추어 볼 때 본건의 경우 동의 여부 선택을 위한 첫 화면에 이미 법정 고지사항이 안내되어 있는 점, 법정 고지사항을 게재하는 부분과 이용자의 동의 여부를 표시할 수 있는 부분은 서로 밀접하게 배치되어 있는 점, 재유도 창에는 '확인'과 '취소' 버튼의 각 효과에 대하여 명확히 고지되어 있어 통상의

6) 구체적으로, 개인정보의 수집·이용을 위한 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 내용'을(제15조 제2항), 제3자 제공을 위한 동의를 받을 때에는 '개인정보를 제공받는 자', '개인정보를 제공받는 자의 개인정보 이용 목적', '제공하는 개인정보의 항목', '개인정보를 제공받는 자의 개인정보 보유 및 이용 기간', '동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용'을(제17조 제2항), 각 정보주체에게 알려야 한다.

합리적인 분별능력을 가진 이용자라면 충분히 '확인' 버튼을 클릭함으로써 자신이 상품 소개 등을 위한 개인정보 처리에 동의하게 된다는 사실을 인지할 수 있었을 것으로 보이는 점[7] 등에 비추어 볼 때, 동의를 받는 방법이 다소 미흡했음은 별론으로 하더라도 개인정보 처리에 관한 동의 자체가 없었다고 단정할 수 있는지 의문이 남는다.

Ⅳ • 개인정보 보호책임자(CPO) 내부통제

개인정보법 제31조에 따라 개인정보처리자는 원칙적으로 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자(CPO)를 지정하여야 하고(제1항), CPO는 '개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축' 업무를 수행하며(제3항 제4호), 개인정보처리자는 CPO가 업무를 독립적으로 수행할 수 있도록 보장하여야 한다(제6항).[8]

본건 제재에서 개보위는 적법한 동의 없이 개인정보가 수집·이용된 만큼 본건을 개인정보의 오·남용 사안으로 판단하고, CPO가 그 방지를 위한 내부통제시스템 구축 의무를 소홀히 하였다고 지적한 것으로 보인다. 즉 동의 절차는 개인정보 처리의 핵심적인 절차임에도 CPO의 검토나 통제 없이 위와 같은 동의 구조가 설계되었다는 점에서 CPO가 형식적으로만 존재하거나 독립적으로 업무를 수행하지 않고 있다고 판단한 것이다.

Ⅴ • 과징금 산정 기준 및 절차

개인정보법상 과징금은 전체 매출액의 3%를 초과하지 않는 범위에서 부과할 수 있다(제64조의2 제1항). 다만 신용정보법[9]과는 달리, 개인정보법은 "전체 매출액에서 위반행위와 관련이 없는

7) 다만 일부 보험사의 재유도 창의 경우 '미동의시 서비스를 제공받을 수 없다'는 취지로만 안내되어 있고, 제시된 '동의', '미동의' 버튼의 효과에 대한 안내도 없어, 이용자로서는 '동의' 버튼의 효과가 개인정보 처리에 대한 동의인지, 재유도 창에 제시된 안내 문구 내용 자체에 대한 동의인지를 명확히 인지하지 못하였을 가능성이 있다.

8) CPO의 독립성 보장을 위해, 개인정보처리자는 ① 개인정보 처리와 관련된 정보에 대한 CPO의 접근을 보장하고, ② CPO가 개인정보 보호 계획의 수립·시행 및 그 결과에 관하여 정기적으로 대표자 또는 이사회에 직접 보고할 수 있는 체계를 구축하며, ③ CPO의 업무 수행에 적합한 조직체계를 마련하고 인적·물적 자원을 제공해야 한다(개인정보법 제31조 제9항, 동법 시행령 제32조 제6항).

9) 신용정보법은 제42조의2 제1항에서 '전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.'라고 규정하고 있는 한편, 개인정보법 제64조의2 제2항과 같이 위반행위와 관련이 없는 매출액을 제외하도록 하는 규정을 두고 있지 않다.

매출액을 제외한 매출액"을 기준으로 과징금을 산정하도록 절충 조항을 두고 있다(제64조의2 제2항). 이렇게 '전체 매출액에서 위반행위와 관련 없는 매출액을 제외한 매출액'에 '위반의 중대성에 따라 구분되는 과징금의 산정비율(부과기준율)'을 곱해 산출한 금액이 과징금 산정의 기준금액이 되며, 산정된 기준금액에 1차 조정, 2차 조정 및 부과과징금의 결정 단계를 거쳐 구체적인 금액의 조정 또는 과징금의 부과 여부가 결정된다(개인정보법 제64조의2 제6항, 동법 시행령 제60조의2 제6항 [별표 1의5]).[10)]

본건 제재로 4개 보험사에 대하여 과징금이 부과되었는데,[11)] 아직 이에 관한 개보위의 심의·의결서가 공시되지 않은 관계로 구체적인 산정 방식을 파악하기는 어려우나 위 기준 및 절차를 참고할 수 있을 것으로 보인다.

Ⅵ. 시사점 및 대응방안

본건 제재는 금융기관의 개인정보 처리라 하더라도 신용정보법상 개인신용정보에 해당하지 않는 경우에는 개인정보 분야의 기본법인 개인정보법의 적용 대상이 되고 개보위가 조사 및 처분을 할 수 있다는 점을 개보위의 입장에서 분명히 하였다는 데 의의가 있다.

한편 향후 타 보험사들을 대상으로 본건 제재와 유사한 쟁점을 중심으로 한 조사가 이루어질 가능성도 배제할 수 없는 바, 타 보험사들의 입장에서는 본건 제재 시 지적된 사항을 참고하여 기존 업무 프로세스를 사전에 전반적으로 점검해 둘 필요가 있을 것으로 보인다. 또한 개보위는 본건 제재를 통해 CPO의 내부통제 미흡을 지적하며, 개인정보 유출을 방지하기 위한 안전조치뿐만 아니라 적법한 개인정보 처리를 위한 내부통제시스템 구축 등 역할을 하여야 한다는 점을 분명히 하였다.

특히 「금융회사의 지배구조에 관한 법률」(이하 '지배구조법')의 2024. 1. 2. 개정으로 보험사는 책무구조도를 2025. 7. 2.[12)] 또는 2026. 7. 2.[13)]까지 금융위원회에 제출해야 하고, CPO는 지배구조법 시행령 [별표 1] 중 '1.아. 개인정보 및 신용정보 등 보호업무와 관련된 책무'와 관련하여

10) 부과기준율, 위반행위의 중대성 판단 시 고려사항, 과징금 조정 시 고려사항 등 기타 구체적인 기준은 위 개인정보법 시행령 제60조의2 제6항 [별표 1의5] 참고
11) H보험 61억 9,800만 원, A보험 27억 1,500만 원, H보험 2억 7,300만 원, M보험 2,170만 원
12) 자산총액 5조원 이상 보험회사의 경우
13) 자산총액 5조원 미만 보험회사의 경우

지배구조법 제30조의2에 따른 내부통제등 관리의무를 부담하게 된다. 그런데 개인(신용)정보 처리 동의의 경우 동일한 양식을 반복 사용하는 특성상 대규모의 고객 피해[14]로 연결될 수 있는 반면, 양식상의 오류는 정기적인 점검만으로도 쉽게 개선이 가능하다는 측면에서, CPO의 관리체계 설계 시 동의서 등 관련 양식에 대한 체크리스트 등을 가능한 한 구체적으로 마련하고 이용자의 자유로운 의사 내지 개인정보 자기결정권 보장의 관점에서 동의권이 실질적으로 보장되도록 설계함으로써 법령 위반 가능성에 대한 점검 및 개선 가능성을 높이는 것이 바람직할 것으로 사료된다. ㄴ

14) '대규모 고객 피해 발생'은 내부통제 관리의무 위반에 대한 제재 시 제재 및 감면 여부를 판단하는 '위법행위 고려요소' 중 하나이다{금융위원회·금융감독원, "금융회사 대표이사 및 임원의 「내부통제 관리의무 위반 관련 제재 운영지침(안)」", 2024. 7.}.