개 인 정 보 보 호 위 원 회

심의·의결

안건번호 제2022-005-027호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2022. 3. 23.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 집합투자사업자로 개인정보를 처리하는「개인정보보호법」(이하 "보호법"이라 함) 제2조제5호에 따른 개인정보처리자로서 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대표자	설립일자	주요서비스	종업원 수	자본금

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021. 9월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 수집 현황

피심인은 고객사를 대상으로 연금상품 판매에 관한 온라인 세미나 참가 신청을 위해 개인정보를 수집하였다.

< 개인정보 수집 현황 >

구 분	항 목	건 수
웹세미나 신청자 정보 (유출파일, 엑셀)	(필수) 성명, 휴대전화번호 (선택) 이메일 주소, 직장명	

2. 개인정보 유출 경위

가. 유출 경위 및 규모

피심인은 온라인 세미나 신청자가 본인의 개인정보가 검색엔진(구글)에서 검색된다는 문의가 접수되어, 내부 확인 과정을 통해 유출 사실을 인지하였다.

이로 인해 신청자의 성명, 휴대전화번호, 이메일 주소, 직장명이 포함된 개인정보가 유출되었다.

나. 유출 경과 및 대응

- ’21.9.23. 외부 인터넷 검색엔진(구글)에서 본인의 개인정보가 검색되고 있다는 온라인 세미나 신청자의 전화를 받고, 홈페이지 개발 업체 수탁사에 문제 확인 및 수정 요청하고, 접속 페이지를 차단 조치함
- ’21.9.24. 개인정보보호 포털에 유출 신고함
- ’21.9.26. 검색엔진(구글)에서 노출 페이지가 검색되지 않고 최종 삭제된 것을 확인함

- ’21.9.27. 관리자페이지 소스 프로그램을 변경하여 노출 페이지 차단 조치함

- ’21.9.28.~10.6. 개인정보 유출 사실 통지 및 홈페이지에 유출 사실 안내문을 게시함

3. 개인정보보호 법규 위반 행위 사실

가. 개인정보처리시스템의 안전성 확보 조치를 소홀히 한 행위

피심인은 연금상품 판매 담당자를 대상으로 온라인 세미나 참가 신청 접수를 위해 웹페이지를 개발한 사실이 확인되었다.

개발 과정에서 일부 관리자페이지가 비인가자의 접근 통제가 허용된 상태(세션값 누락)로 설정되어 있었으며, 검색엔진(구글 IP)이 정보수집(크롤링)[1]을 통해 개인정보가 검색되었던 것으로 확인되었다.

접속 로그기록 확인 결과 검색엔진(구글)이 최초 접근일(’21.7.26. 09:52)부터 차단 조치 확인일(’21.9.26. 17:10)까지 약 2개월간 총 257회(다운로드, 성공 152회/실패 105회) 외부 접근이 허용된 사실이 확인되었다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022.2.7. ‘개인정보 보호법 위반기관 행정처분 사전통지’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 개인정보보호위원회에 선처를 요청하였다.

Ⅲ. 위법성 판단

1. 개인정보처리시스템의 안전성 확보 조치를 소홀히 한 행위

1) 검색엔진의 정보수집(크롤러) 단계는 인터넷에 있는 웹사이트를 주기적으로 방문하여 각종 정보를 자동으로 수집하는데, 이때 웹사이트의 일부 웹페이지가 검색엔진 내 일정기간 동안 보관된다. 가령 주민등록번호 등 개인정보를 포함한 웹페이지가 검색엔진에 수집될 경우 원 사이트에서 해당 웹페이지의 개인정보를 삭제 조치하더라도, 크롤러가 개인정보가 삭제 조치된 웹페이지를 재수집하지 않는 동안 개인정보가 여전히 검색엔진에 검색될 수 있다. 따라서 홈페이지에 개인정보가 잠시라도 업로드 된 경우에는 반드시 해당 노출 내용이 검색엔진에 의해 수집되었는지를 확인하고 검색엔진에 남아 있는 개인정보를 삭제하여야 한다.

가. 관련 법령의 규정

보호법 제29조는 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령이 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하고 있다.

1) 같은 법 시행령 제30조제1항에서는 개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)의 안전성 확보 조치를 하도록 규정하고 있다.

2) 시행령 제30조에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준(위원회 고시)」에서 개인정보처리자의 안전성 확보 조치 내용을 다음과 같이 구체적으로 정하고 있다.

가) 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.(고시 제6조제3항)

나. 위법성 판단

피심인이 취급 중인 개인정보가 열람 권한이 없는 자에게 유출되지 않도록 개인정보처리시스템 등에 접근 통제 등에 관한 조치를 하지 않은 행위는 보호법 제29조 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조 [별표2]「과태료의 부과기준」에 따라 다음과 같이 300만원의 과태료를 부과한다.

가. 기준금액

피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위별 1회 위반에 해당하는 금액 600만원을 적용한다.

< 과태료 부과기준 2. 개별기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
자. 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	**600**	1,200	2,400
계		**600**		

나. 과태료의 가중

피심인의 위반행위는 과태료 부과기준 1. 일반기준 라.에 규정된 가중할 수 있는 사유에 해당하는 사항이 없으므로 가중 없이 기준금액을 유지한다.

다. 과태료의 감경

피심인은 조사기간 중 위반행위를 중지하며 시정 완료한 점, 행위사실을 인정하면서 자료제출·진술 등 조사에 협력한 점 등을 고려하여 과태료 부과기준에 따라 기준금액의 50%인 300만원을 감경한다.

라. 최종 과태료

피심인의 제29조 위반 행위에 대해 기준금액 600만원에서 50%를 감경한 300만원을 부과한다.

< 최종 과태료 산출내역 >

위반조항	위반내용	과태료 금액 (단위 : 만원)			
		기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) =(A+B+C)
법 §29	안전성 확보에 필요한 조치를 하지 않음	600	-	△300	**300**
계		600	-	△300	**300**

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반에 대해서 같은 법 제75조(과태료) 제2항제6호에 의한 과태료를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2022년 3월 23일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(서 명)

위　　원　　강 정 화　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　백 대 용　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　염 홍 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)