개 인 정 보 보 호 위 원 회
심의·의결

안건번호 제2022-005-022호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2022. 3. 23.

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 5,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 비영리 사회공헌 사업을 운영하면서 개인정보를 처리하는 자로서 「개인정보 보호법」(법률 제16930호, 이하 "보호법"이라 함) 제2조제5호에 따른 개인정보처리자이며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대 표	설립일자	매출액('20년)	당기순이익('20년)	종업원 수

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021. 8월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 경위

가. 유출 경과 및 대응

일시		인지 및 대응
’21.8.25.	15:03	신원 미상자가 개발 DB에 접속하여 DB를 삭제
’21.8.26.	10:30	재수탁사 담당자가
’21.8.26.	14:28	백업 데이터를 이용하여 개발 DB를 복구함
’21.8.26.	15:29	모든 해외 IP의 접근을 차단함
’21.8.26.	16:46	개발 DB 차단조치를 실행함
’21.8.26.	16:53	개인정보보호 포털에 신고함
’21.8.26.		개인정보 유출을 통지하고 홈페이지에 공지함
’21.8.28.		재수탁사를 방문하여 사고조사를 진행하고 확인된 문제점에 대해 개선조치를 요청함

나. 유출 규모 및 경위

’21.8.25. 15:03 미국 IP에서 다수의 로그인 실패 기록이 있는 것으로 보아 무작위 대입공격에 의한 무단 접근으로 추정되고, 해당 시간에 해외 IP주소로 데이터 전송 이력이 있었다. 이를 통해 홈페이지 개발 DB에서 성명, 이메일, 연락처 등 최대 명의 개인정보가 유출되었을 것으로 추정된다.

개발 DB 서버의 접속권한에 대한 IP주소가 제한되어 있지 않고 개발 DB에 접속하는 개인정보취급자 계정(root)의 비밀번호가 ‘ ’로 설정되어 있었다.

피심인은 접근통제(웹방화벽 신규 도입, 방화벽 IP 접근통제 설정 등), 접근권한, 접속기록(DB접속 및 운영 로그 기록 생성 설정) 등에 대한 개선조치를 실시하였다.

2. 개인정보보호 법규 위반 행위 사실

가. 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 개발 DB(개인정보처리시스템)에 대한 접속 권한을 IP주소 등으로 제한하지 않았고, 개발 DB에 접속하는 개인정보취급자 계정의 비밀번호를 안전하지 않게 설정하였다. 또한, 개인정보취급자의 개발 DB 접속 여부와 접속하여 수행한 업무내역의 접속기록을 보관·관리하지 않았다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021.10.1. '개인정보보호 법규 위반에 대한 행정처분 사전통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 2021.12.30. 피심인은 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법령의 규정

보호법 제29조는 개인정보처리자는 개인정보가 유출 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하고 있고,

같은 법 시행령 제30조제1항은 개인정보처리자는 법 제29조에 따라 제2호개인정보에 대한 접근 통제 및 접근 권한의 제한 조치, 4호개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 등 안전성 확보 조치를 하여야 한다고 규정하고 있다.

「개인정보의 안전성 확보조치 기준」(고시 제2020-2호) 제5조제5항은 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다고 규정하고 있고,

제6조제1항은 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한하는 기능을 포함한 조치를 하여야 한다고 규정하고 있으며, 제8조제1항은 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다고 규정하고 있다.

나. 위법성 판단

피심인이 개인정보취급자가 안전한 비밀번호를 설정하여 이행하게 하지 않고 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 않은 행위와 개인정보취급자가 개인정보처리시스템에 접속한 기록을 보관하지 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 540만원의 과태료를 부과한다.

가. 기준금액 산정

피심인이 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 기준금액은 1회 위반에 해당하는 600만원을 적용한다.

< 과태료의 부과기준 >

위반행위	근거 법조문	위반횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1200	2400

나. 과태료의 가중

피심인의 제29조에 따른 안전성 확보에 필요한 조치 위반행위의 정도가 중대하여 과태료의 부과기준에 따라 기준금액의 30%인 180만원을 가중한다.

* ①개인정보에 대한 접근 통제 및 접근권한 제한 미조치, ②접속기록 미보관

다. 과태료의 감경

피심인이 위반행위에 대하여 조사기간 중에 일관되게 행위사실을 인정하면서 조사에 적극 협력하였고 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 중에 있는 것으로 인정되므로 기준금액의 40%인 240만원을 감경한다.

라. 최종 과태료

피심인이 보호법 제29조를 위반한 행위에 대해 540만원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반조항	처분조항	기준 금액(A)	가중액 (B)	감경액 (C)	**최종액 (D=A+B+C)**
제29조	제75조제2항제6호	600	180	△240	**540**

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반에 대해서 같은 법 제75조(과태료) 제2항제6호에 의한 과태료 부과를 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 흥 열 (서 명)

위 원 지 성 우 (서 명)