개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

의 안 번 호 제2023-213-248호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2023. 6. 27.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초사실

피심인은 「개인정보 보호법」(이하 '보호법'이라 한다.) 제2조제5호에 따른 개인정보처리자이며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

사업자 등록번호	대표자 성명	주소	직원 수

Ⅱ. 사실조사 결과

개인정보보호위원회는 피심인의 유출신고를 접수받아 사실조사('21. 11. 25. ~ '23. 1. 25.)를 진행하여, 피심인의 개인정보보호 법규 위반행위와 관련된 다음과 같은 사실을 확인하였다.

1. 행위 사실

가. 개인정보 수집 현황

피심인은 ○○○○○종합지원센터 회원정보를 '21. 11. 25. 기준 아래와 같이 개인정보를 수집·보유하고 있다.

구분	수집 항목	건수
회원정보	(필수) 성명, ID, 비밀번호, 이메일, 전화번호, 주소 (선택) 자녀명, 자녀생년월일, 자녀성별	31,528건

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

○○○○○종합지원센터 회원정보 31,528명의 개인정보가 유출되었으며, 성명, ID, 비밀번호, 이메일, 전화번호, 주소 등이 포함되어 있었다.

2) 유출 인지 및 대응

일시	피심인의 유출인지·대응 내용
'20.12.31.	한국인터넷진흥원의 안내로 개인정보 유출 인지
'21. 1. 1.	개인정보 유출신고
'21. 1. 3.	개인정보 유출 관련 SQL 인젝션 공격 취약점 및 웹셸 업로드 취약점 조치
'21. 1. 4.	개인정보 유출통지(이메일), 홈페이지에 유출 안내문 게재

3) 유출 경위

'○○○○○종합지원센터 홈페이지'에서 비밀번호 등 사용자가 입력하는 값에 대하여 SQL 구문과 같은 입력값을 제한하지 않고, 게시판에 업로드가 가능한 파일에 대해 검증하지 않아, 해커가 웹취약점을 이용하여 회원정보 31,528건을 탈취하였다.

다. 개인정보의 취급.운영 관련 사실관계

1) 개인정보의 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 '○○○○○종합지원센터 홈페이지'에서 비밀번호 등 사용자가 입력하는 값에 대하여 SQL 구문과 같은 입력값을 제한하지 않고, 게시판에 업로드가 가능한 파일에 대해 검증하지 않는 등 접근통제 조치를 하지 않아 해커에게 회원정보 31,528건이 유출되었으며, 비밀번호 등을 암호화하여 저장할 때 안전하지 않은 알고리즘을 적용하여 저장한 사실이 있다.

2. 예정된 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 1. 26. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 2. 9. 위반 사실을 인정하고 위반사항에 대해 전부 시정을 완료하였다는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”고 규정하고 있다.

같은 법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근통제 및 접근권한의 제한 조치(제2호), 개인정보를 안전하게 저장할 수 있는 암호화 기술의 적용(제3호) 등의 안전성 확보 조치를 하여야 한다.”고 규정하고 있다.

고시 제6조제3항은 “개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다.”고 규정하고 있으며, 고시 제7조제5항은 “개인정보처리자는 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.”고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전조치 의무를 소홀히 한 행위

피심인이 ‘○○○○○종합지원센터 홈페이지’에서 비밀번호 등 사용자가

입력하는 값에 대하여 SQL 구문과 같은 입력값을 제한하지 않고, 게시판에 업로드가 가능한 파일에 대해 검증하지 않는 등 접근통제 조치를 하지 않아 회원들의 개인정보가 열람권한이 없는 제3자에게 유출된 것은 보호법 제29조, 같은 법 시행령 제30조제1항, 고시 제6조제3항을 위반한 것이며,

피심인이 비밀번호 등의 개인정보를 암호화하여 저장할 때 안전하지 않은 알고리즘을 적용하여 저장한 행위는 보호법 제29조, 같은 법 시행령 제30조제1항, 고시 제7조제5항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치 의무 위반(접근통제)	보호법 §29	§30①	개인정보처리시스템에 대한 접근통제를 하지 않은 행위 (고시§6③)
			개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암화화하여 저장하지 않은 행위 (고시§7⑤)

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반행위에 대한 과태료는 같은 법 제75조제2항제6호, 같은 법 시행령 제63조의 [별표2] 「과태료 부과기준」에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 아래의 위반행위에 대해 1회 위반에 해당하는 금액 600만원을 적용한다.

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

「개인정보 보호법 위반에 대한 과태료 부과기준」('이하 과태료 부과지침') 제8조(과태료의 가중)는 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 동 지침 [별표2]의 가중기준에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

피심인의 보호법 제29조 위반에 대한 과태료는 과태료 부과지침 제8조 [별표2] 가중기준에 따라 위반행위별 각 목의 세부기준에서 정한 행위가 2개인 점을 고려하여 기준금액의 10%인 60만원을 가중한다.

< 과태료의 가중기준(제8조 관련) >

기준	가중사유	가중비율
위반의 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우	기준금액의 50% 이내
	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내

다. 과태료의 감경

과태료 부과지침 제7조는 사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 동 지침 [별표1]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 과태료 부과지침 제7조(과태료 감경)에 따라 의견제출 기간 내 법규 위반행위를 시정 완료한 점, 자료제출 등 조사에 적극 협력한 점을 고려하여 기준금액의 50%인 300만원을 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사 협조·자진 시정 등	1. 과태료의 사전 통지 및 의견 제출 기간 내에 법규 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50% 이내
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 40% 이내

※ 과태료 부과지침 제7조(과태료의 감경기준)에 따라 과태료의 감경은 기준금액의 50%을 초과할 수 없음

라. 최종 과태료

피심인의 보호법 제29조 위반행위에 대해 기준금액에 가중·감경을 거쳐 **360만원의 과태료를 부과**한다.

과태료 처분		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제29조(안전조치 의무 위반)	제75조제2항제6호	600	60	300	**360**

☞ 피심인이 과태료 고지서를 송달받은 날부터 14일 이내에 과태료를 자진납부 하는 경우, 100분의 20을 감경함 (질서위반행위규제법 제18조 및 같은 법 시행령 제5조 준용)

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제75조제2항제6호에 따라 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 재판절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2023년 6월 27일

위 원 장　　지 성 우　(서 명)

위　　원　　강 정 화　(서 명)

위　　원　　염 홍 열　(서 명)