개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2023-016-206호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

(사업자등록번호 :)

피 심 인

대표자

의결연월일 2023. 10. 11.

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 4,200,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법[1]」(이하 "舊보호법"이라 한다.) 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

피심인명	사업자등록번호	대표자 성명	주소	직원 수

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 유출 신고('23. 6. 16.)가 접수되어 개인정보 관리실태에 대한 조사('23. 6. 26. ~ 9. 1.)를 실시하였으며, 피심인의 舊보호법규 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 홈페이지 회원 정보 관리 등을 위해 '23. 8. 30. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

개인정보파일 (시스템명)	수집·이용 항목	수집일	보유건수
홈페이지 회원정보 (대표 홈페이지)		'13.3월~ 현재	

1) 개정된 보호법 시행(2023.9.15.) 이전에 위반행위가 종료된 경우로서 舊개인정보 보호법[법률 제16930호]을 적용

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

대표 홈페이지의 회원 정보 34,288건이 유출되었으며, 유출된 개인정보에는 서명, 학번 및 직번(ID), 비밀번호 등이 포함되어 있었다.

2) 유출 인지 및 대응

일시		피심인의 유출 인지·대응 내용
2022.	7.19.	, 기숙사에서 웹셸 업로드 방식 등으로 개인정보 탈취
	11.15.	교육사이버안전센터, 시스템 취약점 관련 조치 권고(해킹 사실 未인지)
		시스템 취약점 관련 보안 조치, **시정 완료**
2023.	6.13.	경찰청에서 해킹 피해 사실 통보
	6.14.	경찰 보관 중인 자료와 수검기관 DB 대조, **유출 사실 최초 인지**
	6.16.	한국인터넷진흥원에 **유출 신고**
	6.16.	정보주체에게 **유출 통지**(문자)

3) 유출 경위

학생이 ’22. 7. 19. 피심인의 현장실습관리시스템의 특정 소스코드( )에서 입력된 파라미터에 대한 검증이 누락된 점을 이용하여 웹사이트 관리 솔루션의 주요 소스코드를 다운로드하였고, 이를 통해 발견한 데이터베이스 접속 정보 및 파일 업로드 취약점을 이용하여 웹셸을 업로드하는 방식으로 회원정보 테이블에 접근하여 데이터를 다운로드함으로써 개인정보가 유출되었다.

다. 개인정보의 취급·운영 관련 사실관계

1) 개인정보의 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 '대표 홈페이지'의 특정 소스코드에서 입력된 파라미터에 대한 검증을 누락하는 등 시스템 다운로드 취약점에 대한 접근 통제 조치를 소홀히 함으로써, 권한없는 제3자가 웹사이트 관리솔루션의 소스코드를 다운로드할 수 있게 하고, 데이터베이스 연결정보를 발견할 수 있도록 한 사실이 있으며, 경찰 수사 자료(웹셸 업로드 로그 기록) 및 시스템 공격자 노트북에서 발견된 공격코드 및 소스코드, DB 정보 등을 고려할 때 시스템 업로드 취약점에 대한 접근 통제 조치를 소홀히 함으로써 웹셸 업로드를 허용한 것으로 확인된다. 또한 피심인은 학생 및 교직원의 비밀번호를 안전하지 않은 암호알고리즘(MD5)으로 암호화하여 저장한 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 9. 4. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 9. 20. 개인정보보호위원회에 "위반 사실을 시정하였으며 선처를 요청한다"라는 내용의 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 개인정보의 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법 규정

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

또한 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호, 이하 '舊고시') 제6조제3항은 "개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다."고 규정하고 있으며, 제7조제5항은 "개인정보처리자는 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다."라고 규정하고 있다.

나. 위법성 판단

1) 개인정보처리자는 취급중인 개인정보가 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템 등에 접근 통제 등에 관한 조치를 하여야 하나, 피심인이 시스템 취약점 관련 접근 통제 조치를 하지 않아, 권한 없는 제3자의 접근을 허용한 행위는 舊보호법 제29조, 같은 법 시행령 제30조제1항, 舊고시 제6조제3항 위반에 해당한다.

2) 개인정보처리자는 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 하나, 피심인이 안전하지 않은 암호알고리즘(MD5)으로 개인정보를 암호화한 행위는 舊보호법 제29조, 같은 법 시행령 제30조제1항, 舊고시 제7조제5항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊보호법 제29조 위반행위에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조의 [별표2]에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 제29조 위반행위에 대해 1회 위반에 해당하는 과태료인 600만 원을 적용한다.

< 舊보호법 시행령 제63조 [별표 2] - 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 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」(개인정보위 2023. 3. 8. 이하 '舊과태료 부과지침') 제8조(과태료의 가중)는 "사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다"라고 규정하고 있다.

피심인의 舊보호법 제29조 위반행위는 舊과태료 부과지침 제8조의 과태료 가중기준에서 각 목의 세부기준에서 정한 행위가 2개 이상인 경우(+10%)에 해당하며, 법 위반 상태의 기간이 3개월 이상인 경우(+10%)에 해당하므로 기준금액의 20%인 120만 원을 가중한다.

< 舊과태료 부과지침 [별표 2] - 과태료 가중기준 >

기준	가중사유	가중비율
위반의 정도	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내
위반 기간	법 위반상태의 기간이 3개월 이상인 경우	기준금액의 50% 이내

다. 과태료의 감경

舊과태료 부과지침 제7조(과태료의 감경)는 "사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다."라고 규정하고 있다.

피심인은 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 시정 완료하고, 조사 기간 중 일관되게 행위 사실을 인정하면서 자료 제출 등 조사에 적극 협력하였으므로, 舊과태료 부과지침 제7조 [별표1] 감경기준에 따라 기준금액의 50%인 300만 원을 감경한다.

< 舊과태료 부과지침 [별표 1] - 과태료 감경기준 >

기준	감경사유	감경비율
조사 협조·자진 시정 등	1. 과태료의 사전 통지 및 의견 제출 기간이 종료되기 이전에 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

라. 최종 과태료

피심인의 舊보호법 제29조 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 420만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만 원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제29조(안전조치 의무)	법 제75조제2항제6호	600	120	300	**420**

Ⅴ. 결론

피심인의 舊보호법 제29조 위반행위에 대하여 같은 법 제75조제2항에 따라 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.

이상과 같은 이유로 주문과 같이 의결한다

2023년 10월 11일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　김 일 환　(서 명)

위　　원　　김 진 욱　(서 명)

위　　원　　김 진 환　(서 명)

위　　원　　박 상 희　(서 명)

위　　원　　윤 영 미　(서 명)

위　　원　　조 소 영　(서 명)