개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2024-019-244호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (:)

대표자

의결연월일 2024. 11. 13.

주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

   가. 과 징 금 : 193,000,000원

   나. 과 태 료 : 6,600,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 시정조치를 명령한다.

   가. 피심인은 개인정보처리시스템에 침입탐지시스템(IDS), 침입방지시스템(IPS) 등 보안 프로그램을 설치·운영한다.

   나. 피심인은 오라클이 '17. 10월 배포한 보안패치를 개인정보처리시스템에 설치·적용한다.

   다. 피심인은 주민등록번호가 포함된 증빙자료를 암호화 하여 내부 저장공간에 보관한다.

라. 피심인은 가.부터 다.까지의 시정조치를 이행하고, 시정명령 통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 이행 결과나 계획을 제출한다.

3. 피심인에 대하여 다음과 같이 개선을 권고한다.

가. 피심인은 개인정보처리시스템에 대해 개인정보 보호대책 전반에 대한 정비를 실시한다.

나. 피심인은 가.의 개선권고를 이행하고, 개선권고 통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 이행 결과를 제출한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」(이하 '보호법'이라 한다) 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	직원 수

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 유출 신고('24. 1. 30.)에 따라 피심인의 개인정보 관리실태를 조사('24. 3. 5. ~ 5. 30.)하였으며, 피심인의 보호법 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 제공을 위해 '78. 3월부터 아래와 같이 개인정보를 처리하고 있다.

개인정보파일 (시스템명)	수집·이용 항목	수집일	보유건수

나. 개인정보 유출 관련 사실관계

1) 유출 경위

해커가 피심인의 대표 홈페이지*에 존재하는 웹로직 취약점**(CVE-2017-10271)을 악용, 내부 저장공간에 악성파일(웹셸)을 업로드하여 개인정보를 탈취 후 텔레그램에 유포하였다. 해커가 공개한 파일을 분석한 결과, 학생·교직원 등 20명 이상의 주민등록번호를 포함한 5백여명(2천여건) 이상의 개인정보(이름, 학과, 학번, 주소, 연락처, 소속, 사번 등)가 포함되어 있었다.

*

** WLS Security 구성 요소에서 부적절한 사용자 입력 값 처리로 인해 인증되지 않은 공격자가 WebLogic의 권한으로 원격 코드 실행이 가능한 잘 알려진 취약점으로 **관리자 계정에 로그인 없이, 다양한 명령(업로드, 다운로드 등)를 원격 수행 가능**

해커가 업로드한 웹셸(5.jsp)을 통한 다량의 데이터 통신(288.32MB)으로 보이는 웹로그 기록과 피심인 소속 직원과 인터뷰 내용 및 텔레그램에 공개된 파일을 비교해 볼 때, 해당 웹로그 기록은 개인정보 파일이 유출된 정황으로 보인다.

2) 유출 규모 및 항목

피심인의 지출결의서, 증명서 등 240여개 파일에 포함된 개인정보 537명(약 1,950건)이 유출되었고, 유출 항목에는 **주민등록번호(23명)**, 성명, 학과, 학번, 주소, 연락처, 소속, 사번 등이 포함되었다.

3) 유출인지 및 대응

일시			유출 인지·대응 내용
'24	1.27.	18:38	▸ 학과 졸업생 제보로 텔레그램 대학 공격 예고 확인
		20:35	▸ 홈페이지 접근 관련 텔레그램 게시
		20:38	▸ 교육부 사이버안전센터에서 텔레그램 모니터링 중 대학 공격 확인 페이지 탐지 확인하여 통보

일시			유출 인지·대응 내용
		20:44	▸개인정보파일 kr.zip 텔레그램 게시
		22:00	**▸홈페이지 시스템 점검 및 개인정보 유출파일 확인**
		22:17	▸공격 관련 서비스(apache, oracle) 차단 및 WAS 취약점 파일 삭제
		22:24	▸교육부 ECSC 관련 보안 사고 신고
		23:55	▸WAS 취약점 조치 및 홈페이지 웹서비스 재 기동
	1.28.	00:00	▸관련 서비스 모니터링 및 자료 복구 및 파일 위변조 확인
		00:06	▸교육부 사이버 위협 정보공유시스템(ECSC) 사건접수
	1.29.	09:00	▸개인정보 유출 피해 현황 분석 및 모니터링
		13:00	▸ 경찰청 사이버수사대, 국가정보원 현장조사 및 사건 대응
		17:00	▸대학 개인정보보호대책위원회 구성 및 운영
	1.30.	09:30	▸교육부 KERIS, 국가정보원 조사 및 사건 대응
		15:00	**▸개인정보 노출 확인자 메일 통지 및 상황실 대응**
		15:44	**▸개인정보 유출 신고**
	2.1.	09:00	▸개인정보 노출 미확인자 문자 추가 통지

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보의 안전성 확보조치를 소홀히 한 행위

피심인이 구축·운영중인 방화벽(UTM)에 포함되어 있는 웹방화벽(WAF)과 침입방지시스템(IPS) 기능을 설정하지 않았고, 포함되어 있지 않은 침입탐지시스템(IDS)은 포함되지 않았음에도 별도로 설치·운영하지 않은 사실이 있으며, 오라클이 '17.10월 웹로직 취약점 해소를 위해 배포한 보안패치를 현재까지 적용하지 않은 것으로 확인하였다.

결과적으로 해커는 홈페이지에 존재한 웹로직 취약점을 이용하여 내부 저장공간에 악성파일(웹셸)을 업로드할 수 있었고, 피심인은 해커가 웹셸을 업로드 및 이용하기 위해 홈페이지에 불법적으로 접근한 시도를 탐지·차단하지 못하였다.

나. 주민등록번호를 암호화 조치를 통해 안전하게 보관하지 않은 행위

피심인은 주민등록번호가 포함된 강사채용 관련 증빙자료들을 내부 저장공간에 보관하면서 암호화 조치를 현재까지 하지 않고 있다.

Ⅲ. 위법성 판단

1. 관련 법 규정

보호법 제24조제3항은 “개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.”라고, 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 있고, 같은 법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.”라고 규정하면서 “개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치(제3호), 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대해 컴퓨터바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치(제6호)”를 규정하고 있다.

「개인정보의 안전성 확보조치 기준」(개인정보위 고시 제2023-6호, 이하 ‘고시’) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.”라고 하면서 “개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응(제2호)”을 규정하고 있고, 고시 제9조제2항은 “개인정보처리자는 악성 프로그램 관련 경보가 발령된 경우 또는 사용중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.”라고 규정하고 있다.

또한, 보호법 제24조의2제2항은 “개인정보처리자는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보의 안전성 확보 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무) 중 접근통제 및 악성프로그램 등 방지]

피심인이 웹방화벽(WAF)과 침입방지시스템(IPS) 기능을 설정하지 않았고, 침입탐지시스템(IDS)을 설치·운영하지 않았으며, ’17.10. 오라클이 배포한 보안패치를

적용하지 않은 행위는 **보호법 제24조제3항과 제29조, 시행령 제30조제1항제3호 및 제6호, 고시 제6조제1항 및 제9조제2항 위반에 해당한다.**

나. 주민등록번호를 암호화 조치를 통해 안전하게 보관하지 않은 행위

[보호법 제24조의2(주민등록번호 처리의 제한)제2항]

피심인이 주민등록번호가 포함된 강사채용 관련 증빙자료들을 내부 저장공간에 보관하면서 암호화 조치를 하지 않은 행위는 **보호법 제24조의2제2항 위반에 해당한다.**

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '24. 10. 22. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였고, 피심인은 '24. 11. 6. 개인정보보호위원회에 의견을 제출하였다.

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 보호법 제24조제3항 및 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2제1항 제9호, 시행령 제60조의2 [별표 1의5] 및「개인정보 보호법 위반에 대한 과징금 부과기준」(개인정보위 고시 제2023-3호, 이하 '과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제24조제3항 및 제29조 위반에 대한 과징금은 같은 법 제64조의2 제1항 단서규정과 시행령 제60조의2제2항에 따라, 20억 원을 초과하지 아니하는 범위에서 부과할 수 있다.

나. 기준금액

1) 위반행위의 중대성 판단

'과징금 부과기준' 제8조제1항은 "시행령 [별표 1의5] 2. 가. 1) 및 2)에 따른 위반행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준을 기준으로 정한다."라고 규정하고 있다.

[별표] 위반행위의 중대성 판단기준에 따르면 '위반행위의 중대성의 정도는 고려사항별 부과기준을 종합적으로 고려하여 판단'하고, '고려사항별 부과수준 중 두

가지 이상에 해당하는 경우에는 높은 부과 수준을 적용한다.’라고 규정하고 있으며, ‘고려사항별 부과 수준의 판단기준은 ▲(고의 · 과실) 위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려, ▲(위반행위의 방법) 안전성 확보 조치 이행 노력 여부, 개인정보 보호책임자 등 개인정보 보호 조직, 위반행위가 내부에서 조직적으로 이루어졌는지 여부, 사업주, 대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 개인정보의 유출등과 안전성 확보 조치 위반행위와의 관련성을 포함하여 판단, ▲(위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향) 피해 개인정보의 규모, 위반기간, 정보주체의 권리 · 이익이나 사생활 등에 미치는 영향 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 유출 등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.’라고 규정하고 있다.

피심인의 ▲ 고의·과실, ▲ 위반행위의 방법, ▲ 처리하는 개인정보의 유형, ▲ 정보주체의 피해 규모 및 정보주체에게 미치는 영향 등을 종합적으로 고려하여, **위반행위의 중대성을 ’중대한 위반행위*‘로 판단**한다.

* ①(**고의·과실: 중**) 웹방화벽·IPS 등 보안장비 미설치하였고, 오라클 웹로직 취약점에 대한 보안패치를 적용하지 않은 것은 중과실에 해당하나, 개인정보보호책임자 및 정보화팀을 지정·운영하고 있는 점을 참작함
②(**부당성: 중**) 안전조치의무 위반이 유출에 영향을 끼쳤으나, 조직적 위반 등 내부 관여가 없고, 피심인은 CPO 및 정보화팀을 운영하고 있음
③(**개인정보 유형: 상**) 주민등록번호(23명)
④(**피해규모 및 영향: 하**) 537명의 개인정보만 유출되었고, 2차 피해사례가 없음

2) 기준금액의 산출

’과징금 부과기준‘ 제6조제2항은 “영 제60조의2제2항 각 호의 어느 하나에 해당하여 제1항을 적용할 수 없는 경우에는 영 [별표 1의5] 제2호 가목 2)에 따라 기준금액을 정한다.”라고 규정하고 있다. 피심인의 경우, ’중대한 위반행위‘의 **기준금액을 325,000천 원**으로 한다.

<시행령 [별표 1의5] 2. 가. 2)에 따른 기준금액>

위반행위의 중대성	기준금액
매우 중대한 위반행위	7억 원 이상 18억 원 이하
중대한 위반행위	2억 원 이상 7억 원 미만
보통 위반행위	5천만 원 이상 2억 원 미만
약한 위반행위	5백만 원 이상 5천만 원 미만

다. 1차 조정

'과징금 부과기준' 제9조에 따라, 피심인의 보호법 제29조 위반행위의 기간*이 2년을 초과하여 '장기 위반행위'에 해당하므로, **기준금액의 100분의 50**에 해당하는 **162,500천원을 가산하고,**

* 위반기간: 보안 프로그램 미설치('19.1.~현재) / 보안패치 미적용('17.10.~현재)

위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우(30% 이내)에 해당하고, 공공기관인 피심인의 업무 형태 및 규모에 비해 과중(50% 이내)하다고 판단되어 **기준 금액의 100분의 80에**(최대 90% 감경 가능) **해당하는 260,000천 원을 감경**한다.

라. 2차 조정

'과징금 부과기준' 제10조에 따라, 피심인이 조사에 적극 협력(30% 이내)하여, **1차 조정을 거친 금액의 100분의 15에 해당하는 34,125천 원을 감경**한다.

마. 과징금의 결정

피심인의 보호법 제24조제3항 및 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제64조의2 제1항제9호, 시행령 제60조의2 [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 2) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 **193,000천 원을 최종 과징금으로 결정**한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
•중대한 위반행위 (325,000천 원 적용)	•2년 초과*(50% 이내): 50% 가중 •취득이익 없음(30% 이내) : 30% 감경 •공공기관**(50% 이내) : 50% 감경 (△97,500천 원)	•조사협력(30% 이내) : 15% 감경 (△34,125천 원)	**193,000천원***
⇒ 325,000천 원	⇒ 227,500천 원	⇒ 193,375천 원	

* 위반기간: 보안 프로그램 미설치('19.1.~현재) / 보안패치 미적용('17.10.~현재)

** 대학은 고등교육을 담당하는 공공기관인 점을 감안하여 1차 조정에서 50% 감경 적용

*** 부과과징금이 1억원 이상인 경우 1백만원 단위 미만 절사(과징금 부과기준 §11⑤)

2. 과태료 부과

피심인의 보호법 제24조의2제2항 위반행위에 대해 같은 법 제75조제2항제8호, 시행령 제63조 [별표2] 제2호 카목 및「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보위 '23. 9. 15. 이하 '과태료 부과지침')에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

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 피심인의 보호법 제24조의2제2항 위반행위에 대해 1회 위반에 해당하는 과태료 600만 원을 적용한다.

< 시행령 제63조 [별표 2] - 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
카. 법 제24조의2제2항을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제8호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

과태료 부과지침 제7조(과태료의 가중)는 "당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표3]의 가중기준에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다"라고 규정하고 있다.

과태료 부과지침 제7조에 따라, 피심인의 보호법 제24조의2제2항 위반기간이 2년을 초과하는 경우(30% 이내)에 해당*하므로 **기준금액의 100분의 30**에 해당하는 **180만 원을 가중**한다.

* 위반 기간: '19.3. ~ '24.1.

< 과태료 부과지침 [별표 3] - 과태료의 가중기준 >

기준	가중사유	가중비율
위반기간	1. 법 위반 상태의 기간이 2년을 초과하는 경우	기준금액 30% 이내

2) 과태료의 감경

과태료 부과지침 제6조(과태료의 감경)는 “당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.”라고 규정하고 있다.

피심인은 조사 기간 중 일관되게 행위 사실을 인정하면서 자료 제출 등 조사에 적극 협력(20% 이내)하였으므로, 과태료 부과지침 제6조에 따라, 피심인의 보호법 제24조의2제2항 위반행위에 대해 **기준금액의 100분의 20**에 해당하는 **120만 원을 감경**한다.

< 과태료 부과지침 [별표 2] - 과태료의 감경기준 >

기준	감경사유	감경비율
조사 협조	보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액 20% 이내

다. 최종 과태료

피심인의 보호법 제24조의2제2항 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 **총 660만 원의 과태료를 부과한다.**

< 과태료 산출 내역 >

구분		과태료 부과기준			
		기준금액	가중	감경	계
§24의 2②	적용비중	600만원	30%	△20%	10%
	적용근거		▲법위반 기간 2년 초과 (30%이내) * '19.3. ~ 현재	▲조사 협조(20%이내)	**660만 원**
총계		660만 원			

3. 시정명령

피심인의 보호법 제24조제3항, 제24조의2제2항 및 제29조 위반사항이 현재까지 시정되지 않은 것에 대해 **같은 법 제64조제1항에 따라 시정조치를 명령**한다.

4. 개선권고

피심인은 고등교육기관으로서 높은 수준의 개인정보 보호조치가 필요한 점을 종합적으로 고려, 시스템 특성을 감안하여 개인정보 보호대책 전반을 정비하도록 **보호법 제61조제2항에 따라 개선을 권고**한다.