개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2024-019-245호

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 과징금을 부과한다.

   가. 과 징 금 : 42,800,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 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. 31.)에 따라 피심인의 개인정보 관리실태를 조사('24. 2. 23. ~ 5. 30.)하였으며, 피심인의 보호법 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 제공을 위해 '86. 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 2천여명(4천여건)의 개인정보(이름, 학과, 학번, 휴대전화번호)가 포함된 것으로 확인되었다.

*

** 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(2.jsp)을 통한 다량의 데이터 통신(169.91MB)으로 보이는 웹로그 기록과 피심인 소속 직원과 인터뷰 및 텔레그램에 공개된 파일을 보유중인 파일과 비교해 볼 때, 해당 웹로그 기록은 개인정보 파일이 유출된 정황으로 보인다.

2) 유출 규모 및 항목

피심인이 성적 검증 등을 위해 임시로 보관 중인 성적파일 41개에 포함된 1,953명(약 4,276건)이 유출되었고, 유출 항목에는 성명, 학과, 학번, 휴대전화번호 등이 포함되었다.

3) 유출인지 및 대응

일시			유출 인지·대응 내용
'24	1.23.	14:23	▸ 텔레그램 모니터링을 통해 대학 홈페이지 위·변조 공격 인지
		15:00	▸ 해킹으로 생성된 파일 삭제 및 이상징후 모니터링 실시
	1.29.	14:08	▸ 교육부 사이버안전센터는 개인정보 유출 침해사고 모니터링 중, 학생 개인정보 유출을 확인하여 통보 ▸ **개인정보 유출 인지**
		14:30 ~ 15:00	▸ 개인정보 침해사고에 대한 기관장(총장) 최초 보고 ▸ 개인정보 침해사고 대응반 구성 ▸ 개인정보 침해사고 대응 절차서를 최신화하여 대응 실시
	1.30.	17:48	▸ 홈페이지에 개인정보 유출 안내
		17:50	▸ 홈페이지에 사과문 게시 및 정보주체에게 **유출 통지**(SMS, 이메일 등)
	1.31.	15:10	▸ 개인정보보호 포털에 **개인정보 유출 신고**
		18:00	▸ 교육부 사이버안전센터에서 침해사고에 대한 현장조사 및 사후 조치 (보안정책 추가, 모니터링 강화 등)

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보의 안전성 확보조치를 소홀히 한 행위

피심인은 오라클이 '17.10월 웹로직 취약점 해소를 위해 배포한 보안 패치를 적용하지 않은 사실이 있다. 이로 인해 해커는 홈페이지에 존재한 웹로직 취약점을 이용하여 내부 저장공간에 악성파일(웹셸)을 업로드할 수 있었다.

Ⅲ. 위법성 판단

1. 관련 법 규정

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 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 컴퓨터 바이러스, 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.

2. 위법성 판단

가. 개인정보의 안전성 확보 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무) 중 악성프로그램 등 방지]

피심인이 웹셸 등 **해킹 공격에 대비한 별도의 탐지·차단 정책을 수립·운영하지 않았고,** ’17.10. 오라클이 배포한 보안패치를 적용하지 않은 행위는 **보호법 제29조, 시행령 제30조제1항제6호, 고시 제6조제1항 및 제9조제2항 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 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2제1항제9호, 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 제29조 위반에 대한 과징금은 같은 법 제64조의2제1항 단서 규정과 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 ▲(고의ㆍ과실) 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 '보통 위반행위*'로 판단**한다.

* ①(**고의·과실: 중**) 불법 침입을 사전 차단하지 못하였고,'17.10월부터 알려진 오라클 웹로직 취약점에 대한 보안패치를 적용하지 않았으나, 웹방화벽· IPS 등 보안장비를 운영하면서 외부 해킹에 대한 이상징후를 자체적으로 인지하여 초동대처한 점을 참작함
②(**부당성: 중**) 안전조치의무 위반이 유출에 영향을 끼쳤으나, 조직적 위반 등 내부 관여가 없고, 피심인은 CPO 및 개인정보 보호 인력을 운용하고 있음
③(**개인정보 유형: 하**) 민감정보·고유식별정보 및 인증정보 해당없음
④(**피해규모 및 영향: 하**) 1,953명의 개인정보가 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, '보통 위반행위'의 **기준금액을 87,500천 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 **43,750천원을 가산하고,**

* 위반기간: 보안패치 미적용(’17.10.~’24.11.7.)

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 70,000천 원을 감경**한다.

라. 2차 조정

‘과징금 부과기준’ 제10조에 따라, 피심인이 조사에 적극 협력(30% 이내)하였고, 사전통지 및 의견제출 기간 내에 시정을 완료(30% 이내)한 점을 고려하여, **1차 조정을 거친 금액의 100분의 30에 해당하는 18,375천 원을 감경**한다.

마. 과징금의 결정

피심인의 보호법 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 **42,800천 원을 최종 과징금으로 결정**한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
•보통 위반행위 (87,500천 원 적용)	•2년 초과*(50% 이내): 50% 가중 •취득이익 없음(30% 이내) : 30% 감경 •공공기관**(50% 이내) : 50% 감경 (△26,250천 원)	•조사협력(30% 이내) 시정완료(30% 이내) : 30% 감경 (△18,375천 원)	**42,800천원***
⇒ 87,500천 원	⇒ 61,250천 원	⇒ 42,875천 원	

* 위반기간: 보안패치 미적용(’17.10. ~ ’24.11.7.)

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

*** 부과과징금이 1억원 미만인 경우 1십만원 단위 미만 절사(과징금 부과기준 §11⑤)

2. 개선권고

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