개 인 정 보 보 호 위 원 회

제 2 소 위 원 회

심의·의결

안 건 번 호 제2025-212-279호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 국방부 (사업자등록번호 : 106-83-03216)

서울특별시 용산구 이태원로 22

대표자 김선호

의결연월일 2025. 6. 25.

주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

   가. 과 태 료 : 4,200,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 개선을 권고한다.

   가. 피심인은 민간 웹호스팅 또는 클라우드서비스를 이용하고 있는 소관 개인정보처리시스템 전체에 대해 웹방화벽(WAF), 침입탐지시스템(IDS) 및 침입차단시스템(IPS) 등 보안 프로그램 옵션을 선택·적용하고 있는지 점검하고 미흡사항을 개선할 것

   나. 피심인은 상기 시스템에 대해 문서에 의한 위탁, 위탁사실 점검 및 수탁자에 대한 교육 이나 관리·감독 등 보호법 제26조의 내용을 이행하고 있는지 점검하고, 미흡사항을 개선할 것.

다. 피심인은 가.부터 나.의 개선권고를 이행하고, 통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 이행 결과를 제출할 것.

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 「정부조직법」에 따른 중앙행정기관으로, 「舊 개인정보보호법」(법률 제16930호, '20. 8. 5. 시행, 이하 '舊 보호법') 제2조제6호가목에 따른 공공기관에 해당하고, 같은 조 제5호에 따른 개인정보처리자로서 일반 현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	직원 수
국방부	106-83-03216	김선호	서울특별시 용산구 이태원로 22	1,037명

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 특수임무수행자보상심의위원회 홈페이지에 해킹 공격을 받아 개인정보가 유출되었다고 신고('24. 8. 14.)함에 따라 개인정보 취급·운영 실태 및 舊 보호법 위반 여부를 조사('24. 2. 19. ~ '24. 10. 30.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 유출 관련 사실관계

1) 유출 경위

신원 미상의 자는 특수임무수행자보상심의위원회 홈페이지(　　)에 존재한 SQL인젝션과 파일 업로드 취약점을 악용하여 DB에 저장된 회원정보를 탈취한 것으로 추정된다.

분석에 활용된 로그자료 현황

- 웹서버 로그('23. 5. 14. ~ '23. 8. 11.) 및 웹방화벽 로그('22.11.11. ~ '23. 8. 11.)
- 웹방화벽 로그에는 대표 홈페이지 관련 로그가 포함되어 있지 않음

로그분석 결과

- ('23. 5. 16. ~ 8. 8.) 29개의 IP로 33회 SQL인젝션 테스트를 수행
- ('23. 8. 2. 18:38) 홈페이지*에 SQL인젝션 공격 → DB내 테이블 및 회원정보 탈취

  * 공격대상 홈페이지 주소:

2) 유출 내용

DB에 저장된 홈페이지 회원 6,414명의 아이디, 비밀번호, 휴대전화번호, 이름, 가입일자, 이메일, 생년월일, 전화번호, 우편번호, 주소 등이 유출되었다.

3) 유출인지 및 대응

피심인은 '23. 8. 10. 18:00경 사이버사령부 작전센터로부터 개인정보가 유출됐다는 연락을 받고, '23. 8. 11. 09:20경 사이버사령부가 확보한 유출자료와 홈페이지 회원정보를 비교·분석한 결과 개인정보가 유출되었음을 인지하였다. 피심인은 같은 날 15:00경 홈페이지 운영을 중단하였고, '24. 9. 20. 폐쇄하였다. 피심인은 '23 8. 14. 14:00경 개인정보보호 포털에 유출 신고를 하였고, 14:10 경 특수임무수행자보상심의위원회 홈페이지에 유출 공고문을 게시하고, 문자메시지와 이메일 등을 통해 정보주체에게 유출 사실을 통지하였다.

3. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 '25. 1. 8. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '25. 1. 21. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 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 있으며, 같은 법 시행령(대통령령 제30892호, ’20. 8. 5. 시행, 이하 ‘舊 시행령’) 제30조제1항은 “개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(2호)”, “개인 정보를 안전하게 저장 · 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(3호)”를 규정하고 있다.

한편, 위 법령에 따른 안전성 확보조치에 관한 세부 기준을 정한 「개인정보의 안전성 확보조치 기준」(개인정보위 고시 제2021-2호, 2021. 9. 15. 시행, 이하 ‘고시’) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.”면서 “개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(1호)”과 “개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응(2호)”를 규정하고 있고, 같은 조 “제3항은 “ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.”라고 규정하고 있으며, 제7조제2항은 “개인정보처리자는 비밀번호 및 생체인식정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 안전조치의무 위반

[舊 보호법 제29조(안전조치의무) 위반]

피심인이 '05. 1. 22. ~ '23. 8. 11. 동안 홈페이지를 운영하면서 기본 웹호스팅 서비스 외에 웹방화벽 형태의 침입탐지 및 차단 유료 서비스를 별도로 신청하지 않고, 웹 어플리케이션의 입력값 및 웹 어플리케이션에 업로드되는 첨부파일에 대한 검증 조치를 하지 않았으며, 홈페이지 회원의 비밀번호를 웹서버에 평문으로 저장한 행위는 舊 보호법 제29조, 같은 법 시행령 제30조제1항, 고시 제6조제1항·제3항 및 제7조제2항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조 위반행위에 대하여 같은 법 제75조제2항제6호 및 舊 시행령 제63조 [별표 2] 제2호자목에 따라 과태료를 부과하되, 각 위반행위에 대한 과태료 액수는 「舊 개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보위 지침, '23. 3. 8. 시행, 이하 '舊 과태료 부과지침')에 따라 다음과 같이 산정한다.

가. 기준금액

舊 보호법 시행령 제63조의 [별표 2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 피심인의 舊 보호법 제29조 위반행위에 대해 1회 위반으로 보아 과태료 부과 시 기준금액을 600만 원으로 한다.

< 과태료 부과기준 >

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

나. 과태료의 가중 및 감경

1) 과태료의 가중

舊 과태료 부과지침 제8조제1항은 “사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 2]의 가중기준에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.”라고 규정하고 있다.

피심인의 舊 보호법 제29조 위반행위는 홈페이지 개설 당시인 ’05. 1. 22.부터 약 18년 6개월이 경과한 ’23. 8. 11.까지 계속되었다. 또한, ①피심인은 보안 프로그램 옵션 적용 등 접근통제 조치를 하였다고 볼 수 없고, ②비밀번호 암호화 등 개인정보를 안전하게 저장하는 데 필요한 조치를 하였다고도 볼 수 없으므로 舊 과태료 부과지침 [별표 2] 제2호의 가중기준 중 ‘위반기간’(법 위반상태의 기간이 3개월을 초과하는 경우) 및 ‘위반의 정도’(2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우)에 따라 기준금액 600만 원의 20%인 120만 원을 가중한다.

< 과태료의 가중기준 >

기준	가중사유	가중비율
위반의 정도	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내
위반기간	법 위반 상태의 기간이 3개월을 초과하는 경우	기준금액의 50% 이내

2) 과태료의 감경

舊 과태료 부과지침 제7조제1항은 “당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 1]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 홈페이지 운영을 중단하는 등 위반행위를 중지·시정한 점, 조사기간 중에 일관되게 행위사실을 인정

하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 점을 고려하여 舊 과태료 부과지침 제7조제1항에 따라 기준금액의 50%(최대)인 300만 원을 감경한다.

< 과태료의 감경기준 >

기준	감경사유	감경비율
조사협조·자진시정 등	1. 과태료의 사전통지 및 의견제출 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

다. 최종 과태료

피심인의 舊 보호법 제29조 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 **420만 원의 과태료를 부과**한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무(접근통제) **위반**	600만 원	120만 원 (기준금액의 20%)	300만 원 (기준금액의 50%)	**420만 원**

2. 개선권고

재발방지를 위해 피심인에게 민간 웹호스팅 또는 클라우드서비스를 이용하고 있는 소관 개인정보처리시스템에 대해 전수 점검 하고, 미흡사항을 개선하도록 舊 보호법 제61조제2항에 따라 개선권고한다.

3. 결과 공표

舊 보호법 제66조제1항 및 「舊 개인정보보호위원회 처분 결과 공표기준」(개인정보위 지침 2020. 11. 18. 시행) 제2조(공표요건)에 따라, 피심인의 舊 보호법 제29조 위반행위는 위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(5호)에 해당하므로 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표

한다. 다만, 개정된 「개인정보 보호위원회 처분결과 공표기준」(2023. 10. 11. 개인정보 보호위원회 의결)에 따라 공표 기간은 1년으로 한다.

개인정보 보호법 위반 행정처분 결과 공표

개인정보 보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1	국방부	舊 보호법 제29조	안전조치의무 위반	2025. 6. 25.	과태료 420만 원

2025년 6월 25일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 舊 보호법 제29조 위반행위에 대하여 같은 법 제75조, 제61조제2항 및 제66조제1항에 따라 과태료 부과, 개선권고 및 공표를 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

2025년 6월 25일

위 원 장 김 진 환 (서 명)

위 원 김 일 환 (서 명)

위 원 김 휘 강 (서 명)