개 인 정 보
보 호 위 원 회
제 2 소 위 원 회

심의·의결

안 건 번 호 제2025-209-222호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2025. 5. 14.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 7,200,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반 내용 및 처분 결과를 피심인 홈페이지에 공표명령한다.

가. 피심인은 처분 등에 대한 통지를 받은 날부터 1개월 이내 당해 처분 등을 받은 사실 등을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 6분의1 크기로 2일 이상 기간 동안(휴업일 포함) 게시할 것

나. 피심인은 원칙적으로 표준 공표 문안을 따르되, 공표 문안 등과 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 개인정보보호위원회와 협의하여 정할 것

이 유

Ⅰ. 기초 사실

피심인은 비영리사단법인으로서 학술강연 및 교류, 학술지 발간 등을 목적으로 홈페이지를 운영하는 「개인정보 보호법」[1](이하 '보호법')에 따른 개인정보처리자에 해당하며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 해커가 피심인이 운영하는 홈페이지의 관리자페이지 내 회원의 개인정보를 다운로드한 사실을 인지한 피심인이 유출신고('23.10.24.)해옴에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 '24. 1. 19.(자료제출일) 기준 아래와 같이 개인정보를 수집하여 보관하고 있다.

1) 법률 제19234호, 2023. 3. 14. 일부개정, 2023. 9. 15. 시행

< 개인정보 수집현황 >

구 분	수집 항목	기간	규모(명)

나. 개인정보 유출 관련 사실관계

해커*는 알 수 없는 방법으로 획득한 피심인의 홈페이지 관리자계정 정보를 이용하여 관리자페이지에 접속('23.10.8., 19:18~26, 19:04~12)한 후 관리자페이지를 통해 첨부파일을 업로드**하고, 이용자 정보 및 각종 첨부파일을 다운로드('23.10.8. 19:46~)하였다.

* (IP주소) 8.210.140.67(싱가포르), 103.241.72.45(중국)

** 해커가 웹쉘 파일 업로드 공격을 시도했으나 첨부파일이 업로드된 폴더에 실행권한이 부여되지 않아 실행되지 않았음

1) (유출 내용) 홈페이지 회원 5,322명의 개인정보*

* 성명, 소속, 아이디, 생년월일, 성별, 직위, 전화번호, 휴대폰번호, 주소 등

2) (유출 인지 및 대응) 인지 후 72시간을 경과하여 유출 통지 및 신고

일 시	피심인의 유출 인지·대응 내용
'23.10.13.	피심인이 홈페이지 관리자페이지 메일링 리스트에서 수상한 메일을 확인하여 홈페이지 관리업체에 문의 ※ 관리업체는 해킹을 의심하여 관리자계정 비밀번호 변경을 권고
'23.10.17. 16:22	홈페이지 관리업체는 해커가 회원정보를 다운받은 사실을 메일을 통해 피심인에게 통보
'23.10.18. 오후	피심인은 해당 메일 확인 및 개인정보 **유출 인지**
'23.10.23.	회원정보 유출과 관련된 상황에 대해 대책 논의 ※ 피심인은 외부 학술대회 기간 중('23.10.18.~20.) 내부 업무를 진행하지 못하여 행사 이후에 조치 및 대응하였다고 소명
'23.10.24. 18:23	개인정보 포털에 **유출 신고** ※ 피심인은 홈페이지 관리자페이지 로그인 시 학회 사무국과 관리업체 내부 IP에서만 접근할 수 있도록 조치('23.10.25.)
'23.10.26. ~ 11.15.	유출 회원 대상 개인정보 **유출 통지**(이메일) ※ 홈페이지 공지사항 게재

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 홈페이지를 운영하면서 외부에서 개인정보취급자가 관리자페이지에 접속하는 경우 IP주소 등으로 접근을 제한하거나 안전한 접속수단 또는 인증수단을 적용하지 않은 상태로 관리자페이지를 운영한 사실이 있다.

나. 정당한 사유없이 72시간을 경과하여 유출 신고 및 통지한 행위

피심인은 ’23. 10. 18. 오후에 유출 사실을 인지하였으나, 정당한 사유 없이 72시간을 경과하여 ’23. 10. 24.에 유출 신고하였고, ’23. 10. 26.에 유출 통지한 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 ’24. 9. 19. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 10. 7. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 보호법 제29조는 “개인정보처리자는 개인정보가 분실ㆍ도난ㆍ유출ㆍ위조ㆍ변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적ㆍ관리적 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령[2] 제30조제1항제2호나목은 “개인정보에 대한 접근 권한을 제한하기 위한 ‘정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한

2) 대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행

인증수단 적용 기준의 설정 및 운영’의 조치를 해야 한다.”라고 규정하고 있다.

한편, 개인정보의 안전성 확보조치 기준[3](이하 ‘안전성 확보조치 기준’이라 한다.) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(1호)’, ‘개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응(2호)’의 기능을 포함한 조치를 하여야 한다.”라고 규정하고 있으며,

제6조제2항은 “개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.”라고 규정하고 있다.

나. 보호법 제34조제1항은 “개인정보처리자는 ‘유출등이 된 개인정보의 항목(1호)’, ‘유출등이 된 시점과 그 경위(2호)’, ‘유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보(3호)’, ‘개인정보처리자의 대응조치 및 피해 구제절차(4호)’, ‘정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처(5호)’의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.“라고 규정하고 있고, 제34조제3항은 “개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.”라고 규정하고 있다.

시행령 제39조제1항은 “개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조 및 제40조에서 “유출등”이라 한다)되었음을 알게 되었을 때에는 서면등의 방법으로 72시간 이내에 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한

3) 개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 일부개정, 2023. 9. 22. 시행

다. 다만, ‘유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우(1호)’, ‘천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우(2호)’의 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다.“라고 규정하고 있고,

제40조제1항은 “개인정보처리자는 ‘1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우(제1호)’, ‘민감정보 또는 고유식별정보가 유출등이 된 경우(제2호)’, ‘개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우(제3호)’로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 법 제34조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 같은 조 제3항 전단에 따른 전문기관에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인이 홈페이지를 운영하면서 개인정보취급자가 외부에서 관리자페이지에 접속하는 경우 IP 주소 등으로 접근을 제한하거나 안전한 접속수단 또는 인증수단을 적용하지 않은 상태로 운영한 행위는 보호법 제29조, 같은 법 시행령 제30조제1항제2호, 안전성 확보조치 기준 제6조(접근통제) 위반에 해당한다.

나. 개인정보 유출 통지·신고를 소홀히 한 행위

[보호법 제34조(개인정보 유출 등의 통지·신고)제1항·제3항]

피심인은 ’23. 10. 18.에 개인정보 유출 사고가 발생한 사실을 인지하였음에도 불구하고 정당한 사유 없이 72시간을 경과하여 ’23. 10. 26.에 유출 통지한 행위는 보호법 제34조제1항 및 시행령 제39조제1항을 위반에 해당하며, ’23. 10. 24.

에 유출 신고한 행위는 보호법 제34조제3항 및 시행령 제40조제1항을 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과징금 면제

「개인정보 보호법 위반에 대한 과징금 부과기준」[4](이하 '과징금 부과기준') 제11조제2항제2호는 "제10조에 따라 산정된 과징금이 '2백만원 이하인 경우(가목)', '산정된 과태료 금액보다 적은 경우(위반행위가 법 제75조에 따른 과태료 부과 대상이 되는 행위인 경우에 한한다)(나목)'의 어느 하나에 해당하는 경우에는 제10조에 따라 산정된 과징금을 면제할 수 있다."라고 규정하고 있다.

피심인의 보호법 제29조 위반행위는 같은 법 제64조의2제1항제9호, 시행령 제60조의2 [별표 1의5]에 따라 과징금 부과 대상이다.

다만, 산정된 과징금이 200만 원 이하로, ▲유출된 개인정보 중 민감정보, 고유식별정보가 없고, ▲현재까지 정보주체에게 명확히 식별된 피해가 없는 점 등을 고려하여 보호법 제64조의2제1항제9호, 시행령 제60조의2 [별표 1의5] 및 과징금 부과기준 제11조제2항제2호가목에 따라 과징금을 면제한다.

2. 과태료 부과

피심인의 보호법 제29조, 제34조제1항과 제34조제3항 위반행위에 대한 과태료는 같은 법 제75조제2항제5호·제17호·제18호, 시행령 제63조 [별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[5](이하 '과태료 부과기준')에 따라 다음과 같이 부과한다.

가. 기준금액

시행령 제63조 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료

4) 개인정보 보호법 위반에 대한 과징금 부과기준(개인정보보호위원회 고시 제2023-3호, 2023. 9. 15. 시행)
5) 개인정보보호위원회 지침, 2023. 9. 15. 시행

처분을 받은 사실이 없으므로 제29조, 제34조제1항 및 제34조제3항 위반에 대해서는 1회 위반에 해당하는 과태료인 600만 원을 각각 기준금액으로 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		1회	2회	3회 이상
아. 법 **제29조**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 **안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제5호	600	1,200	2,400
노. 법 **제34조제1항**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 **정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우**	법 제75조 제2항제17호	600	1,200	2,400
도. 법 **제34조제3항**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 **보호위원회 또는 전문기관에 신고하지 않은 경우**	법 제75조 제2항제18호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) (과태료의 가중) 과태료 부과기준 제7조제1항은 “당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료 부과기준 [별표3] 과태료의 가중기준(▲위반의 정도, ▲위반기간, ▲조사방해, ▲위반주도)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.‘라고 규정하고 있고, 제7조2항은 ’[별표3]의 각 기준에 따른 과태료 가중 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 가중하되, 기준금액의 100분의 50을 초과할 수 없다.”라고 규정하고 있다.

피심인의 보호법 제29조 위반행위는 위반 기간이 2년을 초과*한 경우에 해당하므로 기준금액의 30%를 가중한다.

* ‘21.1.18.(홈페이지 운영 개시) ~ ‘23.10.25.(IP차단)

피심인의 제34조제1항 및 제34조제3항 위반행위는 과태료 부과기준 제7조 및 [별표3] 과태료의 가중기준에 해당하지 않아 가중없이 기준금액을 유지한다.

2) (과태료의 감경) 과태료 부과기준 제6조제1항은 “당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료 부과기준 [별표2]의 감경기준(▲당사자 환경, ▲위반정도, ▲개인정보처리자의 업무형태 및 규모, ▲개인정보

보호인증, ▲자율규제규약 등, ▲개인정보 보호활동, ▲조사협조, ▲자진시정 등, ▲피해회복·피해확산방지, ▲자진신고)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다. 다만, 과태료를 체납하고 있는 경우는 제외한다.”라고 규정하고 있고, 제6조제2항은 “[별표2]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 감경하되, 제2호 1) 및 2)에 해당하는 사유가 각 2개 이상 해당되는 경우에는 기준금액의 100분의 50을 초과할 수 없고, 최종 합산 결과 기준금액의 100분의 90을 초과할 수 없다.”라고 규정하고 있다.

피심인의 경우, 과태료 부과기준 제6조 및 [별표2] 과태료의 감경기준에 따라 보호법 제29조, 제34조제1항 및 제34조제3항 위반행위에 대하여 ‘비영리법인인 점(30%이내)’, ‘사전통지 및 의견제출 기간 내에 위반행위를 시정 완료한 경우(20%이내)’, ‘일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료를 제출 또는 진술하는 등 조사에 적극적으로 협력한 경우(20%이내)’에 해당하여 과태료 부과기준 제6조에 따라 기준금액의 70%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조, 제34조제1항 및 제34조제3항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 720만 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)
보호법 제29조(안전조치의무)	보호법 제75조(과태료) 제2항제5호	600	180	420	**360**
보호법 제34조(개인정보 유출등의 통지·신고)제1항	보호법 제75조(과태료) 제2항제17호	600	-	420	**180**
보호법 제34조(개인정보 유출등의 통지·신고)제3항	보호법 제75조(과태료) 제2항제18호	600	-	420	**180**
계					**720**

3. 처분결과 공표명령

보호법 제66조제2항 및 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(이하, ‘공표기준’)」[6] 제6조제1항제5호(법 제75조제2항 각 호에 해당하는 위반행위를 3개 이상 한 경우)에 따라 처분 등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분 등을 받은 사실을 피심인의 홈페이지 초기화면 팝업창에 전체화면의 6분의1 크기로 2일 이상 기간 동안(휴업일 포함) 공표하도록 명한다.

이때 공표기준 제7조제1항에 따라 원칙적으로 공표기준 [별표]의 표준 공표문안을 따르되, 공표기준 제8조제3항과 제11조제3항에 따라 공표 문안 등과 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 보호위원회와 협의하여 정한다.

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무), 제34조(개인정보 유출 등의 통지·신고) 제1항 및 제3항 위반에 대하여 같은 법 제64조의2(과징금의 부과)제1항제9호, 제66조(결과의 공표)제2항, 제75조(과태료)제2항제5호·제17호·제18호 및 개인정보보호 법규 위반에 대한 과징금 부과기준 제11조제2항제2호가목에 따라 과징금 면제, 과태료 부과, 공표명령을 의결한다.

6) 개인정보 보호법 위반에 대한 공표 및 공표명령 지침(개인정보보호위원회 지침, 2023. 10. 11. 시행)

이의제기 방법 및 기간

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조제1항에 따라 과태료 부과 통지를 받은 날부터 60일 이내에 개인정보보호위원회에 서면으로 이의제기를 할 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 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납부 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2025년 5월 14일

위 원 장　　김 진 환

위　　원　　김 일 환

위　　원　　김 휘 강