개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2025-217-351호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 숨수면의원

대표자

의결연월일 2025. 9. 10.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 13,500,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

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

이 유

Ⅰ. 기초 사실

피심인은 수면클리닉을 운영하며 수면 질환 진단 등을 위해 환자들의 개인정보를 처리하는 「개인정보 보호법」[1](이하 '보호법') 제2조제5호에 따른 개인정보처리자이다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자	주소	상시 종업원 수
숨수면의원				

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회(이하 '위원회')는 피심인이 CCTV 해킹으로 인하여 병원 환자 및 직원의 개인영상정보가 해외 사이트에 게시된 사실을 인지하고 유출신고(1차: '24.8.6., 2차: '24.12.5.)해옴에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 자료제출일('24.10.31.) 기준, 아래와 같이 개인정보를 수집·보관하였다.

구분	항목	기간	건 수(건)

1) 법률 제19234호, 2023.3.14. 일부개정, 2024.3.15. 시행

나. 개인정보 유출 관련 사실관계

피심인은 수면클리닉을 운영하면서 환자들의 수면다원검사를 위해 검사실에 CCTV를 설치하고 그 영상을 수면 질환 검사 및 진단에 사용하였다. 해커는 해당 CCTV의 NVR에 접속한 후 환자의 개인영상정보를 다운로드하여 유출하였으나, 사고 당시 관련 로그기록 등이 존재하지 않아 정확한 유출 규모 및 경위는 확인되지 않았다.

다만, 해당 NVR은 IpTime 공유기를 통해 외부망에 연결되어 있었고, 공유기에는 포트포워딩으로 외부에서 접속이 가능하여 공격에 노출될 수 있는 환경이었으며, '24.4월 로그를 분석한 결과 불특정 외부인의 악성행위 기록이 확인되었다.

* 숨수면의원 CCTV NVR의 동영상 저장주기는 2주이며, 분석 시점 당시 시스템 로그의 경우 3개월 치만 저장되어 있어 KISA 중소기업 침해사고 피해 지원서비스 현장점검('24.7월) 당시 남아 있는 '24.4월 로그로 분석 진행

또, 피심인은 관리자가 NVR에 접속 시 ID/PW 이외에 IP주소 제한 등 별도 접근통제 조치를 하지 않았고, 당시 관리자 계정의 패스워드는 '소문자 + 숫자 + 기호'로 이루어진 11자리 문자열로, 패스워드 크랙 사이트에 대입해 본 결과 '매우 취약' 상태로 판정된 사실이 있다.

※ (제조사) , (모델명)

※ 사용 모델 의 최신 펌웨어는 버전 v.4.5.001 (빌드버전 201007)으로 이후에 단종되어 펌웨어 업데이트를 지원하지 않았고,

- 숨수면의원의 경우 펌웨어 v3.5.22.(빌드버전 170927)으로, '24.12월 현장조사 시점까지 보안 환경은 해커 등의 침입에 매우 취약한 상태였음(현장 조사 이후 펌웨어 업데이트 조치)

1) (유출 내용) 환자 및 직원 24명의 개인영상정보*

* 검사복 환복 장면 + 얼굴 노출 18명, 얼굴만 노출 3명, 마스크 착용한 얼굴 노출 3명

※ 불법 사이트 업로드 건만 확인 가능, 로그 삭제로 정확한 유출 규모 확인 불가

유출된 파일	유출 항목	유출 규모	수집·보유기간

2) 유출 인지 및 대응

일 시	유출 인지 및 대응 내용
’23. 5. 16. 이전	유출된 영상을 바탕으로 최초 침투시점은 ‘23.5월 이전으로 추정 ※ 유출된 영상 촬영 시점: ’23.5 ~ 6월 추정
’24. 7. 11. 16:52	기자의 제보로 CCTV 영상이 에 게시된 사실을 **인지**함 ※ 총 9명의 CCTV 영상이 결합된 파일
’24. 7. 11. 16:53	KISA 보호나라에 CCTV 영상 해킹 사실을 신고하고 추가 유출 방지를 위해 CCTV와 연결된 외부망 분리 조치
’24. 7. 15. 15:47	KISA 보호나라 ‘중소기업 침해사고 피해지원’ 현장 출동 신청
’24. 7. 22. ~ 8. 5.	KISA 현장 출동 및 분석 수행
’24. 8. 2.	환자로부터 에 CCTV 영상이 유출되었다는 사실을 제보 받음
’24. 8. 2. 15:23	인터넷 장의사를 고용하여 CCTV 영상 삭제 및 추가 유출 모니터링 요청
’24. 8. 5. ~ 8. 6.	KISA 현장점검 결과 조치가 필요한 사항에 대해 후속 조치 완료 ※ CCTV 교체(외부망 연결 해제) 및 관리자 계정정보 변경, 인가된 IP 화이트리스트 적용, 포트 번호 변경 및 비활성화, 로그 파일 백업
’24. 8. 6. 11:29	방송통신심의위원회에 유출 영상이 게재된 사이트 및 디지털 성범죄 신고
’24. 8. 6. 19:13	개인정보 포털에 개인정보 **유출 신고(1차)**
’24. 8. 8. ~ 9. 14.	홈페이지에 개인정보 **유출 사실 공지(1차)** ※ CCTV 영상 속 정보주체의 신원 확인이 어려워, 홈페이지 게시로 대체
’24. 10. 11.	신원이 확인된 정보주체(퇴사 직원)에 개인정보 유출 사실 통지 ※ 유출 사실에 대한 합의 및 합의금 지급(’25. 1. 25.)
’24. 12. 4.	중국 사이트 및 국내 불법 도박사이트에 신규 유출 영상이 게시됨을 **인지**하고 방송통신위원회에 사이트 차단 신고 ※ 총 15명의 CCTV 영상이 결합된 파일
’24. 12. 5.	홈페이지에 개인정보 **유출 사실 공지(2차)**
’24. 12. 6. 17:21	추가로 확인된 영상에 대한 **개인정보 유출 신고(2차)**

3. 개인정보의 취급· 운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 환자의 수면 질환 검사 및 진단을 위해 CCTV로 환자의 수면 영상을 촬영하고 이를 진단에 사용하였으며, NVR에 14일간 저장하였다. 해당 NVR은 개인정보

처리시스템임이 분명하나, 피심인은 NVR 관리자 계정의 패스워드를 외부인이 유출하기 쉽고 단순하게 설정한 사실이 있고, 접속 시 IP 주소 등으로 제한*하지 않는 등 개인정보 처리시스템에 대한 안전조치를 소홀히 한 사실이 있다.

* 확인가능한 '24.4월 로그까지 IP 주소를 이용한 접근제한 조치는 적용되어 있지 않았으며, '24.8.7. IP 주소 화이트리스트를 적용함

나. 개인정보 유출 신고 및 통지를 지연한 행위

피심인은 '24. 7. 11. 기자의 제보를 통해 개인영상정보 유출 사실을 인지했음에도, 정당한 사유 없이 72시간을 경과하여 '24. 8. 6. 유출 신고하고 '24. 8. 8. ~ 9. 14. 동안 유출 통지한 사실이 있다.

※ 피심인은 1차 유출 인지 건에 대한 유출 통지는 정보주체 신원 확인 불가로 자사 홈페이지에 유출 사실을 공지하였고, 이후 신원이 확인된 퇴사 직원에 대해 '24. 10. 11. 별도 통지함

※ 2차 유출 인지 건에 대한 유출 신고 및 통지는 72시간 내 정상적으로 이루어짐

4. 처분의 사전통지 및 의견 수렴

가. 피심인 주장

피심인은 본 건 위법사실을 인정하고 있으나, 해당 CCTV는 촬영된 영상이 중국 소재 서버에 주기적으로 백업되고, 본 건 유출은 해당 백업 서버의 계정이 탈취된 것이 원인으로 단순히 해당 CCTV 제품을 설치해 운영하고 있는 피심인에게 온전한 과실 책임을 묻는 것은 부당하며,

유출된 정보는 민감·고유식별정보나 인증정보에 해당하지 않아 과태료 산정 시 다양한 감경 사유가 존재한다는 점 등을 적극 고려하여 선처를 요청하였다.

나. 검토의견

본 건 유출 원인은 시스템 로그가 삭제되어 유출 원인을 명확하게 특정하지 못하였고, '중국으로 백업되는 서버의 계정 유출'은 추측 가능한 다수의 유출 원인 중 하나인 반면, 유출로 이어질 수 있는 피심인의 안전조치 의무 소홀에 대한 과실은 명확하다.

다만, 피심인이 위반행위로 인한 경제적·비경제적 이득을 취하지 아니한 점, 조사에 적극 협력한 점, 사전통지 및 의견제출 기간이 종료되기 전에 위반행위를 중지하는 등 시정을 완료한 점 등을 종합적으로 고려하여 피심인의 주장을 일부 수용한다.

Ⅲ. 위법성 판단

1. 관련 법 규정

「舊 개인정보 보호법」[2](이하 '舊 보호법') 제29조에서는 "개인정보처리자는 개인정보가 분실・도난・유출・위조・변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적・관리적 및 물리적 조치를 하여야 한다."고 규정하고 있다.

「舊 개인정보의 안전성 확보조치 기준」[3](이하 '안전조치 기준') 제5조제5항에 따라 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 하며, 안전조치 기준 제6조제1항제1호에 따라 개인정보 처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보 처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

한편, 보호법 제34조제1항에서는 "개인정보처리자는 개인정보가 분실・도난・유출되었음을 알게 되었을 때에는 지체없이 해당 정보주체에게 유출항목・시점 및 경위 등을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다."고 규정하고 있으며,

같은 법 제34조제3항에서는 "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."고 규정하고 있다.

2) 법률 제16930호, 2020.2.4. 일부개정, 2020.8.5. 시행
3) 개인정보보호위원회고시 제2021-2호, 2021.9.15. 일부개정, 2021.9.15. 시행

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 수면 질환 검사를 위해 검사실 내 CCTV를 설치하고 그 영상을 진단에 이용하면서, CCTV 영상이 저장되는 NVR의 관리자 계정 패스워드를 유추하기 쉽게 설정하고 접속을 IP 주소로 제한하지 않는 등 안전조치를 소홀히 한 행위는 보호법 제29조 및 같은 법 시행령[4](이하 '舊 시행령') 제30조제1항제2호, 안전조치 기준 제5조제5항 및 제6조제1항을 위반한 것이다.

※ 유출이 일어난 시점은 '23.5월경으로 안전조치 의무 위반은 舊 보호법 적용, 유출사고 인지는 '24.7월로 유출 통지 및 신고 의무 위반은 현행 보호법을 적용

나. 개인정보 유출 신고 및 통지를 지연한 행위

[보호법 제34조(개인정보 유출 등의 통지·신고)제1항·제3항]

피심인이 개인정보 유출 사실을 인지하였음에도 정당한 사유 없이 유출 통지 및 신고를 지연한 행위는 보호법 제34조제1항 및 제3항을 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조(안전조치 의무) 및 보호법 제34조(개인정보 유출 등의 통지·신고) 제1항·제3항 위반행위에 대한 과태료는 같은 법 제75조제2항제5호·제17호·제18호, 같은 법 시행령[5] 제63조의 [별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[6](이하 '과태료 부과기준') 에 따라 다음과 같이 부과한다.

※ 舊 보호법 제29조 위반행위에 대해, '질서위반행위규제법' 제3조(법 적용의 시간적 범위)제2항에 따라 과태료 부과 시 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보보호위원회 지침, '23. 9. 15. 시행)을 적용함

4) 대통령령 32813호, 2022.7.19. 일부개정, 2022. 7. 19. 시행
5) 대통령령 제34309호, 2024. 3. 12. 일부개정, 2024. 3. 15. 시행
6) 개인정보보호위원회 지침, 2023. 9. 15. 시행

1) 기준금액

시행령 제63조 [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 舊 보호법 제29조 및 보호법 제34조제1항·제3항 위반에 대해 1회 위반에 해당하는 과태료인 600만 원을 각 기준금액으로 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
아. 법 제23조제2항·제24조제3항·제25조제6항(법 제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·**제29조**(법 제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	舊 보호법 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	보호법 제75조 제2항제17호	600	1,200	2,400
도. **법 제34조제3항**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 전문기관에 신고하지 않은 경우	보호법 제75조 제2항제18호	600	1,200	2,400

2) 과태료의 가중

과태료 부과지침 제7조는 “당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표3]의 가중기준에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.“라고 규정하고 있다.

피심인의 舊 보호법 제29조 위반행위는 ‘위반기간 1년 초과 2년 이내(15% 이내)’ 및 ‘위반행위 2개(15% 이내)’에 해당하여 기준금액의 30%를 가중하고, 보호법 제34조제1항·제3항 위반행위에 대해서는 가중없이 기준금액을 유지한다.

< 과태료 부과기준 [별표3] 제3호>

위반행위별	세부기준
보호법 시행령 제63조 별표2 제2호 아목	나. 영 제30조제1항제2호에 따라 개인정보에 대한 접근 권한을 제한하기 위한 조치를 하지 않은 경우
	다. 영 제30조제1항제3호에 따라 개인정보에 대한 접근을 통제하기 위한 조치를 하지 않은 경우

3) 과태료의 감경

과태료 부과지침 제6조는 “당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.“고 규정하고 있고, “[별표2]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상 해당되는 경우에는 기준금액의 100분의 50을 초과할 수 없다.“고 규정하고 있다.

피심인의 舊 보호법 제29조 및 제34조제1항·제3항 위반행위에 대해 ’중기업인 경우(15% 이내)‘, ’시정완료(20% 이내)‘에 해당하여 기준금액의 35%를 감경한다.

4) 최종 과태료

피심인의 舊 보호법 제29조 및 보호법 제34조제1항・제3항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만 원)			
위반조항	처분 조항	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
舊 보호법 제29조	법 제75조 제2항제5호	600	180	210	**570**
보호법 제34조제1항	법 제75조 제2항제17호	600	-	210	**390**
보호법 제34조제3항	보호법 제75조제2항제18호	600	-	210	**390**

※ 피심인이 과태료 고지서를 송달받은 날부터 14일 이내에 과태료를 자진납부 하는 경우, 100분의 20을 감경함(질서위반행위규제법 제18조 및 같은 법 시행령 제5조 준용)

2. 결과 공표

피심인의 舊 보호법 제29조 위반에 대하여, 「舊 개인정보 보호위원회 처분결과 공표기준」[7]제2조제8호에 따라 처분 결과를 공표하며, 「개인정보 보호위원회 처분결과 공표기준」[8]에 따라 1년간 공표한다.

7) 개인정보보호위원회 지침, 2020. 11. 18. 시행
8) 개인정보보호위원회 지침, 2023. 10. 11. 시행

개인정보보호법 위반 행정처분 결과 공표 개인정보보호법 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	숨수면의원	舊 보호법 제29조	안전성 확보조치 위반	2025. 9. 10.	과태료 600 만 원
2025년 9월 10일 개 인 정 보 보 호 위 원 회					

Ⅴ. 결론

피심인의 舊 보호법 제29조, 보호법 제34조제1항・제3항을 위반한 행위에 대하여 보호법 제75조제2항제5호・제17호・18호에 따라 총 1,350만 원의 과태료를 부과하고 舊 보호법 제66조에 따른 공표를 의결한다.

이의제기 방법 및 기간

피심인은 이 공표에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

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 9월 10일

위 원 장 김 진 환

위 원 김 일 환

위 원 김 휘 강