

개 인 정 보 보 호 위 원 회

심의 · 의결

안 건 번 호 제2024-002-009호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 한국장학재단 (사업자등록번호 : 104-82-10922)

대구광역시 동구 신암로 125

대표자 배병일

의결연월일 2024. 1. 24.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 8,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 개선을 권고한다.

가. 피심인은 시스템의 특성을 감안하여 각종 불법적인 접근 시도 가능성에 대비할 수 있도록 임계치 분석·조정 등 시스템 보안 정책 전반을 정비한다.

나. 피심인은 연계 서버를 포함한 시스템 전반의 주민등록번호 보관 상황을 점검하고, 주민등록번호를 암호화하여 안전하게 보관한다.

다. 피심인은 가.부터 나.까지의 개선권고에 따른 조치를 이행하고, 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

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

이 유

I. 기초 사실

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

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	직원 수
한국장학재단	104-82-10922	배 병 일	대구광역시 동구 신암로 125	524명

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 유출 신고(23. 6. 27.)에 따라 피심인의 개인정보 관리실태를 조사(23. 6. 27. ~ 10. 27.)하였으며, 피심인의 舊 보호법 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 학자금 관련 업무 처리를 위해 'IT선진화시스템'을 통해 '23.7.19. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

개인정보파일 (시스템명)	수집·이용 항목	수집일	보유건수
고객 기본 정보 (IT선진화시스템)	(필수) 성명, 주민등록번호, 생년월일, 연락처(집), 주소(집), 휴대폰, 이메일 등	'20.3월~ 현재	8,802,095명

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

피심인의 대표 홈페이지 회원 32,599명의 개인정보가 유출되었고, 유출된 정보에는 '성명, 이메일 주소, 집 주소, 휴대전화 번호, 고객 번호'(이상 필수 수집)를 비롯하여, '학자금 대출 신청 현황, 학자금 대출 내역, 학자금 대출 잔액, 장학금 신청 현황, 장학금 수혜내역, 대학생 연합생활관 신청현황, 대학생 연합생활관 입주내역, 나의 기부'(이상 선택 수집) 등이 포함되어 있었다.

한편, 피심인은 「한국장학재단 설립 등에 관한 법률 시행령」 제36조의2에 따라 회원들의 주민등록번호를 처리하고 있으나, 유출된 개인정보 항목에 주민등록번호는 포함되지 않은 것으로 확인된다.

2) 유출 인지 및 대응

일시			피심인의 유출 인지·대응 내용
2023.	6.21.	12:06	중국 IP 이용, 최초 시스템 로그인 시도
	6.25.	22:30	시스템 접속량 비정상 증가 확인, 중국발 1차 공격(IP 42만개) 최초 인지 ※ 통합관리시스템에서 WAS서버 로그 파일시스템 사용률 95% 초과 경고 ⇒ 평소(2GB)보다 로그파일 사이즈(14GB)가 매우 커서 로그 파일 확인, 문제 인지
		23:48	중국발 IP의 비정상 로그인 확인 및 중국 IP 차단
	6.26.	00:19	보안관제시스템 경보 규칙 추가 ※ 해외 단일 IP에서 10초당 10건 이상 접근 시도시 시스템 경고 조치
		13:14	미국 등 해외발 2차 공격(IP 1.4만개) 인지, 해외 IP 전체 차단
		15:15	보안관제시스템 경보 규칙 추가 ※ 계정 잠금 현상(로그인 5회 실패)이 10분당 20회 이상 발생시 시스템 경고 조치
	6.27.	02:30	해외 IP 로그인 성공 계정(32,599건) 잠금 처리
		10:06	개인정보위, 한국인터넷진흥원에 유출 신고
		18:05	국내발 3차 공격(IP 6천개) 인지, ID·PW 로그인 방식 폐쇄
	6.27.~6.29.		정보주체에게 유출 통지 (이메일, 문자)
	6.27.~7.27.		대표 홈페이지에 개인정보 유출사실 게재

3) 유출 경위

신원 불상의 자가 불상의 방법으로 아이디와 패스워드를 획득한 후 다른 사이트에서도 이를 동일하게 사용하였을 것이라는 전제하에 프로그램을 활용하여 성공할 때까지 로그인을 시도하거나 패스워드에 약간의 변화를 주어 로그인을 시도하는 ‘크리덴셜 스테핑’ 방식을 이용하여, ‘23. 6. 21. ~ 6. 27. 피심인의 홈페이지에 불법적으로 접근하였고, 국내외 441,464개의 IP를 통해 총 21,037,622회 로그인을 시도하여 36,748회(중복 제거시 32,599회) 로그인에 성공(성공률 0.17%)하였다.

이 과정에서 1분당 홈페이지 로그인 시도 횟수가 최대 14,440회(1초당 240회)까지 증가하였고, 중국발 트래픽량이 평소('23년 1~8월중 일평균 384,685 패킷)보다 최대 36배(6.25. 13,847,468 패킷)까지 증가하였으며, ID·PW 입력 오류로 인한 계정 잠김 현상이 평소('23.6.1.~6.20. 일평균 78.8회)보다 68배(6.21. 5,418회)까지 증가하는 등 비정상적인 로그인 시도가 급증하였다. 로그 분석 결과 홈페이지의 '로그인 페이지'(개인정보 없음)와 '마이페이지'(개인정보 13종)에 동일하게 접근한 이력이 확인되었고, 여타 페이지에 접근한 사실은 확인되지 않았다.

4) 피심인의 소명 내용

피심인은 불법적인 접근 및 침해사고 방지를 위해 DDos 방어, 웹방화벽, 침입방지 시스템(IPS), 보안관제 시스템(ESM), 통합관리시스템(EMS) 등을 운영하고 있으며, 시간당 일정 수준 이상의 트래픽이 발생할 경우 경고하는 보안 정책을 적용하고 있으나, 공격자가 이례적으로 많은 수의 IP(44만여개)를 사용하여 정상적인 웹 호출과 유사한 속도(10초 이내 평균 17개 내외의 패킷 전송)로 일정한 간격을 두고 접속을 하는 등 정상적인 로그인으로 위장하였기 때문에 트래픽량에 기반한 피심인의 보안 정책으로는 탐지하지 못하였다고 소명하였다.

또한 해당 공격 시기는 '23년 2학기 1차 국가 장학금 신청 기간(5.23.~6.22.)으로 시스템 접속량이 급증하는 시기였던 점, 학자금 신청 업무의 경우 학생들이 대학 공용시설에서 동일한 공인 IP를 사용하여 접속하는 경우가 많은 점 등 단일 IP 접속량 증가를 반드시 이상 행위로 간주하기 곤란한 시스템 특성이 있다고 소명하였다.

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보의 안전성 확보조치를 소홀히 한 행위

피심인은 1분당 홈페이지 로그인 시도 횟수가 최대 14,440회(1초당 240회)까지 증가하였고, 중국발 트래픽 량이 평소보다 최대 36배까지 증가하였으며, ID·PW 입력 오류로 인한 계정 잠김 현상이 평소보다 68배까지 증가하는 등 비정상적인 로그인 시도가 급증하였음에도, 로그인 URL을 대상으로 대량의 로그인을 시도하는 IP 등을 탐지·차단하는 정책을 적용하지 않아 이를 탐지하지 못한 사실이 있다.

이로 인해 최초 공격이 시작된지 4일이 지나 로그 파일시스템 사용률 초과 경고를 받고서야 이상행위 발생을 인지하고 IP 주소 분석 및 차단 등 대응을 진행하였으나, 인지 시점에 신원 불상의 자는 이미 로그인을 33,504회 성공한 사실이 있으며, 피해 발생 이후 피심인은 ‘로그인 5회 실패로 잠금 상태가 된 계정이 10분당 20개 이상 발생할 경우 탐지’하는 정책을 적용하고 ID·PW를 이용한 로그인 절차를 폐쇄한 사실이 있다.

나. 주민등록번호를 안전하게 보관하지 않은 행위

피심인은 대출 심사 및 소득분위 확인을 위해 행정안전부 주민등록시스템과 연계하여 주민등록정보 및 주민등록등본정보를 수신(일 1회)하고 있으나, 시스템 연계서버(IP: 192.168.*.101)에 주민등록번호를 암호화하지 않고 평문으로 저장한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 11. 1. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였고, 피심인은 2023. 11. 15. 개인정보보호 위원회에 “위반 사실을 인정하고 모두 시정하였으며 선처를 바란다”는 내용의 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 있고, 같은 법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.”라고 규정하면서 “개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)”를 규정하고 있다.

「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호, 이하 ‘舊 고시’) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.”라고 규정하면서 “개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응(제2호)”을 규정하고 있다.

舊 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

[舊 보호법 제29조(안전조치의무) 중 접근통제]

개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해

시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하고 대응하여야 하며, 이러한 보호조치를 이행하였는지 여부는 보편적으로 알려져 있는 정보보안의 기술수준, 개인정보처리자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹 기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등 사정을 종합적으로 고려하여 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다.(대법원 2018. 1. 25. 선고 2014다203410 판결 참조)

크리덴셜 스테핑은 국제웹보안표준기구(OWASP)에 '15. 2월부터 보고되어 왔던 해킹 유형이다. 이와 관련, 보편적으로 DB 로그파일의 아이디, IP주소, 로그인 시간, 성공/실패, 접속 URL 등을 실시간으로 파악한다거나, 전체 사용자의 로그인 시도 횟수, 성공/실패한 로그인 횟수, 로그인 성공/실패율을 실시간으로 확인하는 것은 기술적으로 구현 가능하며, 사용자가 탐지 룰을 설정하는 방법에 따라 설정한 임계치를 넘어가는 각종 IP주소를 실시간으로 보여주도록 하는 것도 기술적으로 구현 가능하다. 또한 주기적으로 로그를 사후 확인하여 심층적으로 분석하는 것도 가능하며, 이를 통해 하루 최대 정상적인 로그인 시도 건수를 분석하고 동일 IP에서 초당 또는 분당 접속하는 최대 건수를 확인하여 그에 맞는 보안 탐지 정책을 시스템에 적용할 수 있다.

피심인은 DDos 방어, 웹방화벽, 침입방지 시스템(IPS), 보안관제 시스템(ESM), 통합관리시스템(EMS) 등을 운영하고 있으며, '해외 단일 IP에서 5분에 패킷 300건 이상 발생시 경고', '단일 IP에서 방화벽을 통과한 통신 중 1분에 패킷 2,000건 이상 발생시 경고' 등 보안관제 정책 173개, 웹 방화벽 정책 282개, 침입방지 시스템 정책 6,364개, DDos 차단 시스템 정책 604개 등을 운영하고 있으나, 본건과 같은 크리덴셜 스테핑 공격에 대해 효과적으로 대응할 수 있도록 '동일한 IP에서 일정 횟수 이상 로그인을 시도하거나, 실패할 경우 접속을 제한'하는 형태의 보안 정책은 도입·적용하지 않았으며, 웹 서비스로 전달되는 요청

패킷 전체를 모니터링하는 시스템은 갖추지 않았다고 소명하였다. 실제 6.21. ~ 6.25. 비정상적인 접근 시도가 이어졌으나 피심인의 보안 정책으로 탐지하지 못하였고, 로그 파일이 쌓여 사용률 95% 초과 경고를 받고서야 이상 행위 여부를 분석·탐지한 사실이 확인된다. 피심인은 피해 발생 이후 별도 경제적 비용 발생 없이 ‘로그인 실패 관련 보안 정책’(로그인 5회 실패로 계정잠금 현상 10분당 20회 이상 발생시 경고)을 추가로 도입하여 국내발 3차 공격을 탐지해낸 사실이 확인된다.

또한 시기적으로 국가 장학금 신청 기간과 일부 겹쳐 시스템 접속량이 증가하는 시기였고, 주 사용자인 학생들이 대학 공용시설 등에서 동일한 공인 IP로 접속하는 경우가 많다고 하더라도, 단시간 내 대량의 접속 실패를 동반하는 것은 정상적인 이용자들의 접속 형태가 아님을 충분히 의심할 수 있으며, 시스템의 특수성을 감안하더라도 홈페이지 로그인 횟수가 1초당 240회까지 증가하거나, ID·PW 입력 오류로 인한 계정 잠김 현상이 평소의 68배까지 증가한 것 등은 비정상적인 접근으로 간주하여 대응하여야 할 사안으로 판단된다.

IP 주소 대역에 대한 보안 정책을 강화할 경우 정상적인 접근까지 공격으로 잘못 탐지할 여지가 없는 것은 아니나, 피심인은 본건 개인정보파일을 통해 총 8,802,095명의 개인정보를 취급하고 있고 해당 홈페이지를 통한 6개월 평균 서비스 이용자 수가 1,068,000명에 달하는 등 공공기관 중에서도 높은 수준의 보호조치가 필요하며, 취급하는 개인정보에는 성명·주소 등 기본 사항 외 학자금 대출 신청 현황, 학자금 대출 내역 등 유출될 경우 보이스피싱과 같은 2차 피해에 취약한 금융 관련 정보도 포함되어 있어 불법적인 접근을 탐지·차단할 필요성이 더욱 크므로, 오탐 가능성 및 서비스 편의성 저하 등을 이유로 보안 정책 ‘룰 세팅’ 수준을 완화하는 것은 적절하지 않다고 판단된다.

결국 크리덴셜 스티핑 공격에 대한 방어 여부는 보안 ‘룰 세팅’을 어떤 수준으로 하느냐에 달려 있는데, 시스템의 특성을 감안하여 초당 로그인 시도가 증가하는 시기 및 횟수 등에 대한 분석을 통해 관련 항목들을 실시간으로 관제할

수 있는 기능을 구현하거나, 시스템 보안 정책 임계치 조정 또는 정책 변경 등 방법을 검토하거나, 비정상 접속 의심 계정에 대한 비밀번호 초기화, 캡차 (CAPTCHA, 봇에 의한 공격을 차단하기 위해 문자, 부호 등을 입력하여 인증하도록 하는 기술) 또는 2차 인증절차 도입 등의 조치가 있었다면 본건과 같은 피해 발생을 회피할 가능성이 있었다고 판단된다. 상기 사정들을 종합적으로 고려할 때 피심인이 사회통념상 합리적으로 기대 가능한 정도의 보호조치 의무를 다하였다고 보기 어렵다.

위와 같은 사유로 피심인이 1분당 홈페이지 로그인 시도 횟수, 중국발 트래픽량, ID·PW 입력 오류로 인한 계정 잠금 현상 등 비정상적인 로그인 시도가 급증 하였음에도 이를 탐지하지 못한 행위는 舊 보호법 제29조, 같은 법 시행령 제30조제1항, 舊 고시 제6조제1항을 위반한 것이다.

나. 주민등록번호를 안전하게 보관하지 않은 행위

[舊 보호법 제24조의2(주민등록번호의 처리 제한)제2항]

개인정보처리자는 취급하는 주민등록번호를 암호화하여 안전하게 보관하여야 하나, 피심인이 대출 심사 및 소득분위 확인을 위해 행정안전부 주민등록시스템을 통해 수신하는 주민등록번호를 시스템 연계서버(IP: 192.168.*.101)에 암호화하지 않고 평문으로 저장한 행위는 舊 보호법 제24조의2제2항을 위반한 것이다.

IV. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조 및 제24조의2제2항 위반행위에 대해 같은 법 제75조제2항제6호·제4의3호, 같은 법 시행령 제63조의 [별표2] 및 「舊 개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보위 2023. 3. 8. 이하 ‘舊 과태료 부과 지침’)에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊보호법 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 제29조 및 제24조의2제2항 위반행위에 대해 1회 위반에 해당하는 과태료인 1,200만 원(각 600만 원)을 적용한다.

< 舊보호법 시행령 제63조 [별표 2] - 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
카. 법 제24조의2제2항을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제4의3호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

舊 과태료 부과지침 제8조는 “사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준 (▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다”라고 규정하고 있다.

피심인의 舊 보호법 제29조 및 제24조의2제2항 위반행위는 舊 과태료 부과지침 제8조의 과태료 가중기준에 해당하지 않아 기준금액을 유지한다.

2) 과태료의 감경

舊 과태료 부과지침 제7조는 “사전통지 및 의견제출 결과와 당사자의 위반 행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]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 위반행위를 시정 완료하고, 조사 기간 중 행위 사실을 인정하면서 자료 제출 등 조사에 적극 협력하였으므로, 舊 과태료 부과지침 제7조 [별표1] 감경기준에 따라 기준 금액의 30%인 360만 원을 감경한다.

< 과태료 부과지침 [별표 1] - 과태료 감경기준 >

기준	감경사유	감경비율	
조사 협조 · 자진 시정	1. 과태료의 사전 통지 및 의견 제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	기준금액 50% 이내	합계 상한
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액 40% 이내	50% 이내

다. 최종 과태료

피심인의 舊 보호법 제29조 및 제24조의2제2항 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 840만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만 원	-	180만 원	420만 원
주민등록번호 처리 제한 위반 (암호화 위반)	600만 원	-	180만 원	420만 원
계	1,200만 원	-	360만 원	840만 원

2. 개선 권고

피심인은 대량의 개인정보를 처리하는 공공기관으로서 높은 수준의 보호조치가 필요하다고 판단되므로 개인정보 보호를 위하여 舊 보호법 제61조제2항에 따라 다음과 같이 개선을 권고한다.

- 가. 피심인은 시스템의 특성을 감안하여 각종 불법적인 접근 시도 가능성에 대비할 수 있도록 임계치 분석·조정 등 시스템 보안 정책 전반을 정비한다.
- 나. 피심인은 연계 서버를 포함한 시스템 전반의 주민등록번호 보관 상황을 점검하고, 주민등록번호가 유출되지 아니하도록 암호화하여 안전하게 보관한다.
- 다. 피심인은 가.부터 나.까지의 개선권고에 따른 조치를 이행하고, 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

3. 결과 공표

舊 보호법 제66조제1항 및 「舊 개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 舊 보호법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우에 해당하므로 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호위원회 처분결과 공표기준」(2023. 10. 11. 개인정보보호위원회 의결)에 따라 공표 기간은 1년으로 한다.

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	한국장학재단	舊보호법 제29조	안전조치 의무 위반	2024. 1. 24.	과태료 420만 원 개선권고
		舊보호법 제24조의2 제2항	주민등록번호 처리의 제한		과태료 420만 원 개선권고
2024년 1월 24일 개 인 정 보 보 호 위 원 회					

V. 결론

피심인의 舊보호법 제29조, 제24조의2제2항 위반행위에 대하여 같은 법 제75조 제2항, 제66조제1항에 따라 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

2024년 1월 24일

위 원 장 고 학 수 (서 명)

부위원장 최 장 혁 (서 명)

위 원 김 일 환 (서 명)

위 원 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 조 소 영 (서 명)