개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2024-011-188호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2024. 6. 26.

주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

   가. 과 징 금 : 67,788,000원

   나. 과 태 료 : 11,400,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인 에 대한 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간 공표한다.

이 유

Ⅰ. 기초 사실

방송 프로그램을 제작·공급 하면서 공식 홈페이지( )를 운영하는 피심인은 「舊 개인정보 보호법」[1](이하 '舊 보호법')에 따른 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 포털(privacy.go.kr)에 유출 신고('22. 9. 22.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 5. 1. ~ '23. 10. 4.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 홈페이지 등*을 운영하면서, '23. 6. 16.(자료제출일) 기준 아래와 같이 개인정보를 수집·보관하고 있다.

* 영상 등을 제공하는 메인 홈페이지( )에서는 개인정보를 수집하지 않으며(로그인 기능 없음), 주식정보 사이트( )와 광고 공모전 사이트( )를 통해 개인정보를 수집함

1) 법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행

< 개인정보 수집현황 >

구분	항목	수집일	건수
합 계			

나. 개인정보 유출 관련 사실관계

1) (유출 규모 및 항목) 아래와 같이 이용자의 개인정보가 유출됨

유출 경로	세부 유출 경로	유출항목	유출규모
광고 공모전 페이지		관리자의 아이디, 이름, 비밀번호(MD5), 이메일주소, 부서, 직급	121건 (1인이 복수 계정 생성 가능)
		(이용자 개인정보) 아이디, 이름, 비밀번호(MD5), 닉네임, 생년월일, 성별, 이메일주소(암호화), 전화번호(암호화)	77,931건 (1인이 복수 계정 생성 가능)
		(이용자 계정정보) 아이디, 닉네임, 비밀번호(MD5)	100,903건 (1인이 복수 계정 생성 가능)
	※ 이용자 계정정보 100,903건 중, 이용자 개인정보 77,931건은 중복됨		
		아이디, 이름, 생년월일, 전화번호, 이메일주소, 주소, 학교명, 팀명	6,436건 (1인이 복수 계정 생성 가능)
관리자 페이지		아이디, 이름, 닉네임, 어드바이저명, 어드바이저 상품 가입 기간, 결제 일자·금액, 수강상태, 관리자 메모사항, 담당자명	26,173건

※ 피심인은 유출사고 이후 로그인 체계를 변경(통합 로그인)하고, 본인 인증·확인 이후 1인이 1개의 아이디만 생성 가능하도록 운영함

2) 유출 인지 및 대응

일 시	유출 인지 및 대응 내용
’22. 9. 19. 15:30	을 사칭하여 코인투자를 권유했다는 민원 접수(10건)
’22. 9. 19. 16:25	주식정보 사이트 회원에게 자사 사칭 연락에 대한 주의요망 안내
‘22. 9. 19. 17:00	관리자 페이지 외부 접근을 의심하여 관련 사항 조치
‘22. 9. 20. 11:00	웹서버 접근 로그 분석을 통해 피해 서버 및 SQL 인젝션 공격 확인
‘22. 9. 20. 11:00	외부 전문기관으로부터 분석결과 수신하고 **개인정보 유출 사실 인지**
‘22. 9. 22. 11:47	개인정보 포털에 **개인정보 유출신고 실시**

※ 개인정보위 조사착수 이후 ‘23. 11. 16. 개인정보 유출 개별 통지 완료

3) 유출 경위

해커는 피심인이 운영하는 광고 공모전 페이지( )에 SQL 인젝션 공격(’22. 9. 1. ~ 19.)을 하여 관리자 정보 및 이용자의 개인정보를 획득하였으며, 이후 관리자 페이지( )에 접속하여 주식정보 사이트( )의 유료서비스 이용자 정보를 다운로드하였다.

’22. 9. 8 17:44 해커(61.43.242.68, 한국)가 피심인이 운영하는 광고 공모전 페이지( )에 SQL 인젝션 공격을 통해 DB에 있는 관리자 및 이용자 정보(DB 테이블명·세부항목 및 데이터)를 조회·수집(sqlmap 도구 이용)한 뒤,

’22. 9. 8., ‘22. 9. 10., ’22. 9. 15. 해커가 해외 IP를 통해 관리자 페이지(를 확인하고, SQL인젝션 공격으로 획득한 관리자 계정정보를 이용하여 해당 페이지에 접속(로그인)하였다.

※ 해커는 9.8. 18:16에 관리자 페이지를 확인 후, SQL인젝션 공격으로 획득한 관리자 계정정보를 이용하여 9.10. 18:21에 관리자 페이지에 접속(로그인) 성공함

또한 ’22. 9. 10. 18:25~18:36 해커가 관리자 페이지에 접속하여 주식정보 사이트( )의 유료서비스 이용자 정보를 엑셀로 다운로드하였다.

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 행위

피심인은 ①코로나로 인해 '21. 3. 16. ~ '22. 9. 27. 동안 정보통신망을 통해 개인정보 취급자가 외부에서 관리자 페이지 접속이 가능하도록 운영하면서 추가 인증 등 없이 ID, PW만으로 접속할 수 있는 상태로 운영하였고,

②관리자 페이지에 대한 접속 권한을 IP주소 등으로 제한하지 않았으며 '18. 11 .6. ~ '22. 9. 27. 동안 '광고 공모전 사이트'에 대해 웹 방화벽 등 보안장비 없이 외부에서 웹서버에 직접 접속이 가능하도록 운영하였다.

또한, ③'18. 11. 6. ~ '22. 9. 22. 동안 '광고 공모전 사이트' 내 일부 페이지( )에 SQL 인젝션 공격을 방지하기 위한 조치(입력값 검증 등)를 누락하고 운영한 사실이 있다.

피심인은 '21. 7. 8. ~ '22. 9. 27. 동안 개인정보 취급자가 관리자 페이지를 통해 조회한 DB 접속기록을 보관하지 않고 운영한 사실이 있다.

피심인은 안전하지 않은 일방향 암호화 알고리즘인 MD5로 이용자 및 개인정보 취급자의 비밀번호를 암호화하여 저장·운영한 사실이 있다.

나. 불필요하게 된 개인정보를 파기하지 않은 행위

피심인은 '12. 12. 4. ~ '22. 9. 16. 동안 회원탈퇴를 신청한 회원(2,482명)의 개인정보를 파기하지 않고 보관한 사실이 있다.

다. 개인정보 유출 통지를 소홀히 한 행위

피심인은 유출 신고는 하였으나 이용자에게 자사를 사칭한 연락에 대한 주의사항 안내·공지만 하고 개인정보 유출사실을 통지하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’23. 11. 3. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’23. 11. 3., ‘24. 1. 26., ’24. 5. 28. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 있다.

같은 법 시행령[2](이하 ‘舊 시행령’) 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위해 ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ’그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제48조의2제1항제3호는 “개인정보에 대한 불법적인 접근을 차단하기 위해 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인 · 감독(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있으며, 제48조의2제1항제4호는 “개인정보가 안전하게 저장·전송될 수 있도록 ‘비밀번호의 일방향 암호화 저장(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

舊 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

舊 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 舊 개인정보의 기술적·관리적 보호조치 기준[3](이하 ‘舊 기술적 보호조치 기준’)

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행
3) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15. 시행

제4조제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.”라고 규정하고 있고, 제4조5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(1호)’하고, ‘개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(2호)’하는 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있으며, 제4조9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

또, 제5조제1항은 “정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인 · 감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.” 라고 규정하고 있으며,

제6조제1항은 “정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.”라고 규정하고 있다.

나. 舊 보호법 제21조제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.”라고 규정하고 있다.

다. 舊 보호법 제39조의4제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 “유출등”) 사실을 안 때에는 지체 없이 유출등이 된 개인정보 항목(제1호), 유출등이 발생한 시점(제2호), 이용자가 취할 수 있는 조치(제3호), 정보통신서비스 제공자등의 대응 조치(제4호), 이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)를 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는

전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.”라고 규정하고 있다.

舊 시행령 제48조의4제2항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면 등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.”라고 규정하고 있으며, 제3항은 “정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

정보통신서비스 제공자등은 ①정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 하고, ②정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않는 접근을 제한하여야 하며, ③처리 중인 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 하나,

피심인이 ①코로나로 인해 ‘21. 3. 16. ~ ’22. 9. 27. 동안 정보통신망을 통해 개인정보 취급자가 외부에서 관리자 페이지 접속이 가능하도록 운영하면서 추가 인증 등 없이 ID, PW만으로 접속할 수 있는 상태로 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제4항을 위반한 것이고,

②관리자 페이지에 대한 접속 권한을 IP주소 등으로 제한하지 않고, ’18. 11 .6. ~ ’22. 9. 27. 동안 ‘광고 공모전 사이트’에 대해 웹 방화벽 등 보안장비 없이 외부에서 웹서버에 직접 접속이 가능하도록 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제5항을 위반한 것이며,

③’18. 11. 6. ~ ’22. 9. 22. 동안 ‘광고 공모전 사이트’ 내 일부 페이지( )에 SQL 인젝션 공격을 방지하기 위한 조치(입력값 검증 등)를 누락하고 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제9항을 위반한 것이다.

정보통신서비스 제공자등은 시스템 이상 유무 확인 등을 위해 개인정보취급자가 개인정보처리시스템 접속기록을 최소 1년 이상 보존·관리하여야 하나, 피심인이 ’21. 7. 8. ~ ’22. 9. 27. 동안 개인정보취급자가 관리자 페이지를 통해 조회한 DB 접속기록을 보관하지 않고 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제5조제1항 위반한 것이다.

정보통신서비스 제공자등은 비밀번호에 대하여 복호화되지 아니하도록 일방향 암호화하여 저장하여야 하나, 피심인이 이용자 및 개인정보취급자의 비밀번호를 안전하지 않은 일방향 알고리즘인 MD5로 암호화하여 저장·운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제6조제1항 위반한 것이다.

나. 불필요하게 된 개인정보를 파기하지 않은 행위

[舊 보호법 제21조(개인정보의 파기)제1항]

개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 하나, 피심인이 ‘12. 12. 4. ~ ’22. 9. 16. 동안 회원탈퇴를 신청한 회원(2,482명)의 개인정보를 파기하지 않고 보관한 행위는 舊 보호법 제21조제1항을 위반한 것이다.

다. 개인정보 유출 통지를 소홀히 한 행위

[舊 보호법 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항)]

정보통신서비스 제공자등은 개인정보의 유출 사실을 안 때에는 지체 없이 해당 이용자에게 통지하여야 하나, 피심인이 이용자에게 자사를 사칭한 연락에 대한 주의사항 안내·공지만 하고 개인정보 유출 사실을 통지하지 않은 행위는 舊 보호법 제39조의4제1항, 舊 시행령 제48조의4를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	舊 보호법 §29	§48의2① 제2호	• 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 시, 안전한 인증 수단을 적용하지 않은 행위(舊 기술적 보호조치 기준§4④) • 개인정보처리시스템에 대한 접속 권한을 IP 주소등으로 제한하지 않은 행위(舊 기술적 보호조치 기준§4⑤) • 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(舊 기술적 보호조치 기준§4⑨)
			• 개인정보처리시스템 접속기록을 최소 1년 이상 보관하지 않은 행위(舊 기술적 보호조치 기준§5①)
			• 비밀번호 복호화되지 아니하도록 일방향 암호화하여 저장하지 않은 행위(舊 기술적 보호조치 기준§6①)
개인정보의 파기	舊 보호법 §21①	-	• 보유기간 경과, 개인정보 처리 목적 달성 등 불필요하게 된 개인정보를 파기하지 않은 행위
개인정보 유출등의 통지·신고에 대한 특례	舊 보호법 §39의4①	§48조의4	• 개인정보 유출 통지를 소홀히 한 행위 * 조사착수 이후 '23.11.16. 개별 통지 완료

Ⅳ. 시정조치(안)

1. 과징금 부과

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제5호, 舊 시행령 제48조의11제1항과 제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 舊 개인정보보호 법규 위반에 대한 과징금 부과기준[4]

(이하 '舊 과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 舊 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 舊 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

舊 과징금 부과기준 제5조제1항은 舊 시행령 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 舊 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따라 舊 보호법 제29조(안전조치의무), 舊 시행령 제48조의2(개인정보의 안전성 확보 조치에 관한 특례)를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

舊 과징금 부과기준 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있다. 다만, 舊 과징금 부과기준 제5조제3항 단서에서 위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의

4) 개인정보보호위원회고시 제2022-3호, 2022. 10. 20. 시행

개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당하는 경우 '보통 위반행위'로, 1개 이상 2개 이하에 해당하는 경우 '중대한 위반행위'로 감경하도록 규정하고 있다.

피심인의 경우, SQL 인젝션 공격으로 개인정보가 유출되었으므로, '위반행위로 인해 직접적으로 이득을 취하지 않은 경우(제1호)', '이용자의 개인정보가 공중에 노출되지 않은 경우(제3호)'에 해당하나, 유출된 개인정보가 100분의 5 이내인 경우에 해당하지 않아 '중대한 위반행위'로 판단한다.

3) 기준금액 산출

舊 과징금 부과기준 제4조제1항은 "관련 매출액은 위반 정보통신서비스 제공자 등의 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 직전 3개 사업년도의 연평균 매출액으로 한다."라고 규정하고 있다.

피심인이 공식 홈페이지( )를 통해 발생한 매출을 위반행위 관련 매출로 하고, 직전 3개 사업년도의 연평균 매출액 천 원에 舊 시행령 [별표 1의5] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 천 원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천 원)

구 분	2019년	2020년	2021년	평 균
관련 매출액*				

* 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

< 舊 시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율 >

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	**1천분의 21**
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

舊 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 2년을 초과하므로 '장기 위반행위'에 해당하여 기준금액의 100분의 50에 해당하는 금액인 천 원을 가중하고,

※ 위반기간 : '18.11.6. ~ '22.9.27.

최근 3년 이내 舊 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 천 원을 감경한다.

라. 추가적 가중 및 감경

舊 과징금 부과기준 제8조는 사업자의 위반행위 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중 · 감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따라 피심인이 ▲조사에 적극 협력한 점, ▲개인정보 유출사실을 자진 신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 천 원을 감경한다.

마. 과징금의 결정

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제5호, 舊 시행령 제48조의11, [별표 1의5] 2. 가. 2)(과징금의 산정기준과 산정절차) 및 舊 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 67,788천 원을 최종 과징금으로 결정한다.

< 과징금 산출내역 >

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금
•직전 3개 사업연도 연평균 매출액 (천 원) •연평균 매출액에 2.1%적용 (중대한 위반*)	① 기준금액의 50% 가중 (장기 위반 : 천 원) ② 기준금액의 50% 감경 (최초 위반 : 천 원)	필수적 가중·감경 거친 금액의 20% 감경 (조사협력자진신고 : 천 원)	67,788천 원
⇒ 천 원	⇒ 천 원	⇒ 천 원	

* 중대한 위반 : 고의·중과실이 있는 경우, 매우 중대한 위반행위로 판단하나, ▲위반행위로 직접 취한 이득이 없고 ▲유출된 정보 공중 미노출에 해당하여 중대한 위반행위로 판단함

→ 1개 이상 2개 이하에 해당

2. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무), 제21조(개인정보의 파기)제1항, 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제12호의3, 舊 시행령 제63조, 舊 시행령 [별표2] '과태료의 부과기준' 및 舊 개인정보 보호법 위반에 대한 과태료 부과기준[5](이하 '舊 과태료 부과기준')에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊 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 각 위반행위별 기준금액을 600만 원으로 산정한다.

5) 개인정보보호위원회지침, 2023. 3. 8. 시행

< 舊 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만 원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 **제29조**를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
마. 법 제21조제1항·제39조의6(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제4호	600	1,200	2,400
도. 법 **제39조의4제1항**(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제75조 제2항제12호의3	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 경우, 舊 과태료 부과기준 제8조 및 [별표2] 과태료의 가중기준에 따라 舊 보호법 제29조(안전조치의무) 위반행위는 '법 위반상태의 기간이 3개월 이상인 경우*', '위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상'에 해당하여 기준금액의 20%을 가중하고, 같은 법 제21조(개인정보의 파기)제1항 위반행위는 '법 위반상태의 기간이 3개월 이상인 경우**'에 해당하여 기준금액의 10%를 가중하고, 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위는 '법 위반상태의 기간이 3개월 이상인 경우***'에 해당하여 기준금액의 10%를 가중한다.

* 18.11.6. ~ '22.9.27., ** '12.12.4. ~ '22.9.16., *** '22.9.22. ~ '23.11.16.

2) (과태료의 감경) 舊 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 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.

피심인의 경우, 舊 과태료 부과기준 제7조 및 [별표1] 과태료의 감경기준에 따라 舊 보호법 제29조(안전조치의무) 위반행위는 '과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우', '조사에 적극 협력한 경우', '사업규모가 중기업인 경우'에 해당하여 기준금액의 50%를 감경하고, 같은 법 제29조(개인정보의 파기) 위반행위는 '과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우', '조사에 적극 협력한 경우', '사업규모가 중기업인 경우'에 해당하여 기준금액의 50%를 감경하고, 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위는 '과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우', '조사에 적극 협력한 경우', '사업규모가 중기업인 경우'에 해당하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무), 제21조(개인정보의 파기)제1항, 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,140만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제, 접속기록, 개인정보의 암호화)	600만 원	120만 원	300만 원	**420만 원**
개인정보의 파기	600만 원	60만 원	300만 원	**360만 원**
개인정보 유출등의 통지·신고에 대한 특례	600만 원	60만 원	300만 원	**360만 원**
계				**1,140만 원**

4. 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 경우(제4호), 위반상태가 6개월 이상 지속된 경우(제5호)에 해당하므로 피심인이 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」(2023. 10. 11. 시행)에 따라 공표 기간은 1년으로 한다.

※ 질서위반행위규제법에 근거하여 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023.10.11. 시행)」에 따라 공표기간 1년을 소급 적용

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		舊 보호법* 제29조	안전조치의무	2024. 6. 26.	과태료 부과 420만 원
		舊 보호법* 제21조제1항	개인정보의 파기	2024. 6. 26.	과태료 부과 360만 원
		舊 보호법* 제39조의4 제1항	개인정보 유출등의 통지·신고에 대한 특례	2024. 6. 26.	과태료 부과 360만 원

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2024년 6월 26일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인이 보호법 제29조(안전조치의무), 제34조제1항(개인정보 유출등의 통지·신고)를 위반한 행위에 대하여 같은 법 제64조의2(과징금의 부과)제1항제9호, 제75조(과태료) 제2항제17호, 제66조(결과의 공표)제2항에 따라 과징금 부과, 과태료 부과, 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과징금 부과처분에 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」 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(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2024년 6월 26일

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 이 문 한 (서 명)

위 원 조 소 영 (서 명)