개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2023-012-151호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2023. 7. 12.

주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 원

나. 과 태 료 : 원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

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

이 유

Ⅰ. 기초 사실

운영하는 피심인은 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16930호, 이하 '보호법'이라 한다.)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 개인정보종합포털(privacy.go.kr)에 유출 신고('20. 9. 30.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(. . ~ ' . . .)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 운영하며 '20. 9. 30. 기준으로 아래와 같이 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보		'98. 6. 1. ~ 계속	(유효) (분리보관)
계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
		신원미상의 자(이하, '해커')가 다수 로그인 시도 및 로그인 성공 시 휴면계정 해제 시작
		아이디 도용 의심(휴면계정 해제) 문의 접수
		다수 로그인 시도 IP 확인 및 방화벽 차단
		로그인 시 비밀번호 처리 방식 변경, 해커의 불법 로그인 성공 및 개인정보 접근 건수 확인, 개인정보 유출 사실 인지
		동일 IP의 일일 로그인 수 제한 적용 * 동일 IP에서 1시간 동안 로그인 시도 회수 임계치(30회) 초과시 차단되도록 적용
		개인정보보호 포털에 개인정보 유출신고
		개인정보 유출 관련 이용자 통지(메일)

2) 유출항목 및 규모

이용자 의 개인정보가 유출되었다.

※

3) 유출 경위

해커는 피심인의 홈페이지에 크리덴셜 스터핑 공격을 시도하여 로그인에 성공한 계정의 페이지 등 개인정보를 열람하였다.

※ 해커는 2,179,561회 로그인을 시도(중복제거시 2,002,969건)하여, 51,020회(중복제거시 36,458건)를 성공한 후 개인정보 페이지를 38,218회(중복제거 시 35,076건) 열람함. 이때 사용된 IP 주소는 총 확인됨

해커는 동안 1분당 최대 5,062회, 평균 2,555회의 로그인을 시도하였으며, 피심인이 운영 중인 보안장비 등에서는 대량의 로그인 시도를 탐지·차단하지 못하였다.

※ 공격에 이용된 로그인 시도 횟수는 4,766회 ~ 1,222,845회임

※ 공격에 이용된 IP 주소 중 에 접속한 IP주소는 접속한 것으로 확인됨

피심인은 사고 발생 전까지 '이용자 로그인 페이지'를 대상으로 동일 IP 주소에서 대량으로 로그인을 시도하는 IP 주소 등을 탐지·차단하는 정책을 적절하게 운영하지 않았다.

※ 피심인은 사고 발생 이후 동일 IP주소에서 로그인 시도 횟수 제한 정책을 적용함 (동일 IP주소에서 접속시 해당 IP 차단)

또한, 휴면계정을 해제하는 경우 로그인 후 비밀번호 재입력 이외에 추가적인 인증 절차가 없어, 해커는 공격을 통해 로그인에 성공하면 휴면계정을 해제하고 해당 이용자의 개인정보를 조회할 수 있었다. 다만, 피심인은 휴면계정이 해제되는 경우 등록된 이메일 주소로 휴면계정 해제 사실을 안내하고 있다고 소명한 사실이 있다.

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 사고 발생 당시 크리덴셜 스터핑 공격을 통한 개인정보 유출을 막기 위해 대량으로 로그인을 시도하는 IP 주소 등을 탐지·차단하는 등 불법적인 접근 및 침해사고 방지를 위한 침입탐지·차단 시스템의 운영을 소홀히 하여, ‘

해커가 분당 평균 2,555회 로그인을 시도하였음에도 불구하고 운영 중인 보안장비에서는 이를 탐지한 기록이 없으며,

공격이 발생한 에 휴면계정이 해제되었다는 안내 메일을 받은 이용자가 제기한 민원을 특정 IP 주소에서의 다수 로그인 시도 정황을 확인하였으며, 에 대량 로그인 시도와 불법적인 접근을 시도하는 IP 주소를 확인하여 차단하였고,

에 동일 IP 주소에서 로그인 시도 회수를 제한하는 정책을 적용한 사실이 있다.(동일 IP 주소에서 접속시 해당 IP주소 차단)

또한, 피심인은 해커의 공격 원인을 분석하는 과정에서 에는 평문으로 전송받은 비밀번호는 로그인이 불가하고, 전송받은 비밀번호가 암호화된 경우에만 로그인이 가능하도록 비밀번호 처리방식을 변경하였다.

아울러, 이용자가 휴면계정을 해제하려는 경우 비밀번호 재입력 이외에 추가 인증 없이 휴면계정이 해제되도록 운영하여, 해커 등 권한 없는 자가 휴면계정의 아이디·비밀번호로 로그인에 성공하면 해당 계정 이용자의 아니라 등 조회할 수 있게 시스템을 운영한 사실이 있다. 다만, 피심인은 휴면계정이 해제되는

경우 등록된 이메일로 휴면계정 해제 사실을 안내하는 메일을 발송하고 있다고 소명하였다.

사고 발생 이후, 피심인은 휴면회원이 유효회원으로 전환하려면 캡챠 적용(.), 핸드폰·이메일 등을 통한 추가인증( ) 방식을 적용하는 것으로 휴면회원 해제 절차를 개선하였다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 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 있다.

같은 법 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2021-3호, 이하 '고시') 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리 시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있으며, 제4조제9항은 "정보통신서비스 제공자등은 처리 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라고 규정하고 있다.

고시 해설서는 고시 제4조제5항에 대해 "정보통신서비스 제공자등은 불법적인 접근 및 침해사고 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있고, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 한다고 해설하고 있으며, 접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 것만으로는 부족하며, 신규 위협 대응 및 정책의 관리를 위하여 정책 설정 운영(신규 위협 대응 등을 위하여 접근 제한 정책 및 유출 탐지 정책을 설정하고 지속적인 업데이트 적용 및 운영·관리하는 것) 및 이상 행위 대응(모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응하는 것), 로그 분석(로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 또는 차단하는 것) 등을 활용하여 체계적으로 운영·관리하여야 한다고 해설하고 있다. 또한, IP 주소 등에는 IP 주소, 포트 그 자체뿐만 아니라, 해당 IP주소의 행위(과도한 접속성공 및 실패, 부적절한 명령어 등 이상 행위 관련 패킷)을 포함한다"고 해설하고 있다.

고시 제4조제9항에 관하여는 “정보통신서비스 제공자 등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 및 보안기술을 마련하고 운영 및 관리 측면에서의 개인정보 유·노출 방지조치를 하여야 하며, 인터넷 홈페이지 설계시 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안대책을 마련해야 한다고 해설하고 있다. 이 때, 필요한 보안대책으로는 입력 데이터의 유효성 검증, 에러·오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성, 세션을 안전하게 관리하도록 구성 등과 함께 인증·접근통제 등의 보호조치 적용을 예시로 포함하고 있다. 또한, 홈페이지 개발시 개인정보 유·노출 방지를 위한 보안 기술을 적용하여야 하며, 인터넷 홈페이지 운영·관리 시 개인정보 유·노출 방지를 위한 보안대책 및 기술 적용에 따른 적정성을 검증하고 개선 조치를 하여야 한다”라고 해설하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무 중 접근통제)]

고시 해설서는 고시 제4조제5항에 대해 접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 것만으로는 부족하며, 신규 위협 대응 및 정책의 관리를 위하여 정책 설정 운영(신규 위협 대응 등을 위하여 접근 제한 정책 및 유출 탐지 정책을 설정하고 지속적인 업데이트 적용 및 운영·관리하는 것) 및 이상 행위 대응(모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응하는 것), 로그 분석(로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 또는 차단하는 것) 등을 활용하여 체계적으로 운영·관리하여야 한다고 해설하고 있다.

본 건 유출 사고에 이용된 크리덴셜 스터핑 공격은 해킹기법의 하나로, 해당

공격을 방지하기 위해 동일한 IP 주소에서 일정 시간(예를 들어, 10분) 안에 일정 횟수 이상(예를 들어, 50회) 로그인 시도 시 해당 IP 주소를 일정 시간 동안 차단하거나 또는 비정상적인 로그인 시도를 한 IP 주소에서 특정 아이디로 로그인을 시도하는 경우 해당 아이디로 로그인하는 것을 차단하는 등의 보호정책 설정은 보편적으로 알려진 보안기술이다.

본 건의 경우, 피심인이 보유한 보안기술 및 설치·운영 중인 보안장비 등을 고려할 때, 과도한 접속 성공 또는 실패 등 이상 행위와 비정상적인 로그인 시도 IP 주소를 차단하는 정책은 충분히 적용 가능했던 조치로 판단된다. 실제로 피심인은 사건이 발생하자 동일 IP 주소에서의 로그인 시도 횟수를 제한하는 정책(동일 IP 주소에서 IP 주소 접속 차단)을 적용한 사실이 있다.

고도화된 크리덴셜 스터핑 공격이 아니라 이번 공격과 같이 소수 개의 IP 주소( )에서 대량의 로그인 시도를 하는 일반적인 크리덴셜 스터핑 공격은 보안장비 등에 관련 정책 설정 등으로 차단할 수 있어 추가적인 비용이 발생하지 않거나 발생하더라도 매우 적은 수준인 반면, 해당 정책 적용 시 개인정보 불법 접근을 차단하여 개인정보 유출 및 유출로 인한 사생활 침해 등 피해를 예방한다는 점에서 이용자 개인정보 보호에 따른 효용은 크다고 할 것이다.

본 사건은 해커가 1분당 적게는 1회에서 많게는 5,062회까지 로그인이 시도되었으며, 1분당 평균 2,555회(1초당 평균 42.58회) 로그인을 시도하고, 로그인에 성공한 계정의 개인정보가 유출된 사건으로 피심인은 사고 발생 이후에야 크리덴셜 스터핑 공격을 차단하는 정책을 적용하였으며, 이는 대량의 반복적인 로그인 시도 등 과도한 접속성공 또는 실패 등 이상행위와 비정상적인 로그인 시도 등 불법적인 접근을 차단하기 위한 침입탐지·차단시스템의 운영을 소홀히 한 행위로 보

호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항을 위반한 것이다.

또한, 고시 제4조제9항은 정보통신서비스 제공자등의 내·외부적인 요인 등으로 인하여 개인정보가 외부로 유출되는 사고를 방지하기 위한 목적에서 마련되었다. 고시 제4조제9항의 문언과 입법 목적, 규정 체계 등을 고려하면, 본 조항이 정보통신서비스 제공자등의 의무로 규정하고 있는 조치는 정보통신서비스 제공자등이 취급 중인 개인정보가 내·외부적 요인에 의하여 유출되지 않도록 개인정보처리시스템에 합리적으로 기대 가능한 정도의 기술적 보호조치라고 해석된다.

대법원은 정보통신서비스 제공자등이 고시 제4조제9항에서 정한 보호조치를 다하였는지 여부는 해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, 정보통신서비스 제공자의 업종·영업규모, 정보통신서비스 제공자등이 인터넷 홈페이지 등의 설계에 반영하여 개발에 적용한 보안대책·보안기술의 내용과 실제 개발된 인터넷 홈페이지 등을 운영·관리하면서 실시한 보안기술의 적정성 검증 및 그에 따른 개선 조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹에 의한 개인정보 유출의 경우 이에 실제 사용된 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 정보통신서비스 제공자등이 수집한 개인정보의 내용과 개인정보의 유출로 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 판단하여야 한다고 판시한 바 있다.(대법원 2021. 8. 19. 선고 2018두56404 판결)

고시 해설서, 대법원 판결 등을 볼 때 피심인은 아래에서 보는 바와 같이 취급 중인 개인정보가 유출되지 않도록 고시 제4조 제9항에서 규정하는 기술적 보호조치를 다하였다고 보기 어렵다.

우선, 피심인은 설립되었으나, 부터

이용자 개인정보를 수집하였고, 이후 거쳐 유출사고 발생일인 을 기준으로 사업자다. 또한, 피심인은 을 기준으로 보유한 의 개인정보에는 이용자들이 되어 있다.

피심인은 을 통해서 인지하였으며, 피심인이 제출한 자료에 의하면 공격에 성공한 계정이었다.

피심인은 이용자가 휴면계정을 해제하고자 할 경우, 비밀번호 재입력 이외에 추가적인 인증 없이 휴면계정 해제가 가능하도록 시스템을 운영하였으며, 해커가 크리덴셜 스터핑 공격에 성공하여 로그인하면 별다른 제한 없이 해당 휴면회원의 등 열람할 수 있었다.

휴면계정 해제 등에 사용하는 추가인증은 보편적으로 알려진 보안기술로, 피심인이 보유한 개인정보의 중요도와 정보보호에 필요한 경제적 비용 및 효용의 정도 등을 종합적으로 고려할 때 충분히 적용 가능했던 조치로 판단된다. 피심인도 공격이 발생하고 5일 후인 에 휴면계정 해제시 캡챠를 적용하였고, 캡챠 적용 후 18일이 지난 에는 캡챠 대신 휴대폰·이메일을 활용한 추가인증 절차를 적용한 바 있다.

또한, 피심인이 보유한 개인정보는 포함되어 있어 이용자 입장에서는 정보에 해당하여 개인정보 유출로 인해 이용자가 입게 되는 피해 가능성도 큰 편이라는 점을 고려하면, 서비스 운영·관리 측면에서도 휴면계정 해제시 추가인증 적용이 필요한 조치로 판단된다.

본 사건의 경우, 실제 사용된 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 피심인이 수집한 개인정보가 이 포함되어 있어 이용자 입장에서는 에 해당하여 개인정보 유출로 인해 이용자가 입게 되는 피해 정도 등이 큰 편이라는 점을 종합적으로 고려할 때,

피심인은 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 위험요소를 분석하여 개인정보처리시스템 등에 인증·접근통제 등의 필요한 보안대책을 마련하고 조치하는 등의 고시 제4조제9항에서 규정하는 기술적 보호조치를 다한 것으로 보기는 어렵다고 판단되며, 따라서 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	보호법 §29	§48의2① 제2호	• 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위(고시§4⑤, ⑨)

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제29조 위반에 대한 과징금은 같은 법 제39조의15제1항제5호, 같은 법 시행령 제48조의11제1항과 제4항, [별표 1의5] (과징금의 산정기준과 산정절차) 및 ‘개인정보보호 법규 위반에 대한 과징금 부과기준(개인정보보호위원회 고시 제2022-3호, 이하 ’과징금 부과기준‘이라 한다)’에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 같은 법 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 하여야 하나, “ ”에 해당하여 그 사업 개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

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

보호법 제29조의 안전조치의무를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 ‘매우 중대한 위반행위’로 판단하도록 규정하고 있다.

다만, 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 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당하는 경우 ‘보통 위반

행위’로, 1개 이상 2개 이하에 해당하는 경우 ‘중대한 위반행위’로 규정하고 있다.

피심인의 경우 위반행위로 인해 , 위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 , 에 해당하여 ‘보통 위반행위’로 감경한다.

3) 기준금액 산출

피심인의 관련 매출액은 “ 되지 않은 경우”에 해당하여 사업개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액인 에 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 ‘보통 위반행위’의 부과기준율 1천분의 15을 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2017년	2018년	2019년	평 균
관련 매출액				

※ 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

* 2018. 8. 1. 법인이 신설되어, 2018. 8. 1.부터 환산한 평균값을 적용

<보호법 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

과징금 부과기준 제6조와 제7조에 따라 피심인은 법인을 설립한 월부터 사고가 발생한 까지 크리덴셜 스터핑 공격에 대비한 적절한 접근통제 조치를 하지 않았으며, 사고 발생 이후 해당 접근통제 조치를 하여 위반행위의 기간이 을 초과( )하므로 기준금액의 100분의 인 원을 가중하고, 최근 3년 이내 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 에 해당하는 금액인 천원을 감경한다.

라. 추가적 가중 및 감경

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

이에 따를 때, 피심인이 ▲ , ▲ 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 에 해당하는 원을 감경한다.

마. 과징금의 결정

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

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금

2. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과태료는 같은 법 제75조제2항제6호, 같은 법 시행령 제63조, 같은 법 시행령 [별표2] '과태료의 부과기준' 및 '개인정보 보호법 위반에 대한 과태료 부과기준'(이하 '과태료 부과지침')에 따라 다음과 같이 부과한다.

가. 기준금액

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 1회 위반에 해당하는 과태료인 600만원을 기준금액으로 산정한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 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) 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 '안전성 확보에 필요한 조치를 하지 않은 행위'에 대하여 과태료 부과지침 제8조(과태료 가중기준) 및 〔별표2〕'과태료의 가중기준' 중 ▲법 위반 상태의 기간이 개월 이상( )인 경우로 기준금액의 %를 가중한다.

2) (과태료의 감경) 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 '안전성 확보에 필요한 조치를 하지 않은 행위'에 대하여 과태료 부과지침 제7조(과태료 감경기준)에 따라 ▲

▲

하여 기준금액의 %를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만원			
계				

3. 결과 공표

「개인정보 보호법」 제66조제1항 및 「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 '위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)'에 해당하므로, 피심인에 대한 과태료 부과 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

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	의결일자	처분내용
1		법 제29조	안전조치의무 위반 (접근통제)	2023. 7. 12.	

2023년 0월 00일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반행위에 대하여 같은 법 제39조의15조(과징금의 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항제6호, 제66조(결과의 공표)제1항에 따라 과징금, 과태료, 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

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

피심인은 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.

2023년 7월 12일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　강 정 화　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　백 대 용　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　염 홍 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)