개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2024-011-187호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 에스케이스토아㈜ (사업자등록번호 :)

대표자

의결연월일 2025. 1. 22.

주 문

1. 피심인에 대하여 다음과 같이 과징금, 과태료를 부과한다.

가. 과 징 금 : 1,432,000,000원

나. 과 태 료 : 3,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 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 5일 미만 기간 동안(휴업일 포함) 게시할 것

나. 피심인은 원칙적으로 표준 공표 문안을 따르되, 공표 문안에 관하여 개인정보보호위원회와 미리 문서로 협의해야 하고, 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 개인정보보호위원회와 협의하여 정할 것

이 유

Ⅰ. 기초 사실

피심인은 온라인 쇼핑몰 및 TV 홈쇼핑 서비스를 제공하는 「개인정보 보호법」[1](이하 '보호법')에 따른 개인정보처리자에 해당하며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 신원 미상의 자(이하 '해커') 공격으로 개인정보가 유출된 정황을 인지하고 유출 신고('23. 11. 22.)해옴에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 12. 13. ~ '24. 2. 27.) 하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

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

피심인은 온라인 쇼핑몰 및 TV 홈쇼핑 서비스를 제공하면서 '24. 2. 6.(자료제출일) 기준, 건의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	기간	건수
계			

나. 개인정보 유출 관련 사실관계

해커는 '23. 11. 14. 00:42 ~ 11. 21. 23:19 동안 피심인이 운영 중인 웹사이트(m.skstoa.com(모바일), skstoa.com(PC))의 로그인 페이지( )에 사전에 획득한 계정정보로 '크리덴셜 스터핑*' 공격을 시도하였고, 로그인에 성공한 이용자 계정으로 로그인 후 개인정보가 포함된 페이지를 열람하였다.

* 해커가 다른 방법을 통해 계정·비밀번호 정보를 취득한 후 다른 사이트에서도 이를 동일하게 사용하여 성공할 때까지 로그인을 시도하는 대입 공격

해커는 총 14개의 IP 주소(한국 11개, 중국 2개, 미국 1개)에서 총 44,112,024회 로그인을 시도하였고, 이 중 125,138건(중복 제거)의 이용자 계정으로 접속하였다.

* 해커는 공격 기간('23.11.14.~11.21.) 동일 IP 주소에서 1초당 최대 372회, 평균 92회 로그인 시도

이후, 해커는 125,138건의 계정을 통해 접근한 218개의 웹페이지 중 회원정보 조회 및 상품페이지 등 개인정보를 포함한 5개 웹페이지(URL)에 접근하여 이용자의 개인정보를 열람하였다.

해커의 피심인 웹사이트에 대한 로그인 시도 건수는 공격 기간인 '23. 11. 14. ~ 11. 21. 동안 비공격 기간 대비 약 1,092배 증가하였다.

* 비공격 기간('23.11.6.~11.13.) 일평균 로그인 시도 건수 : 6,690건
  공격 기간('23.11.14.~11.21.) 일평균 로그인 시도 건수 : 7,310,304건(약 1,092배)

한편, 피심인은 회원 정보 수정을 위한 로그인 정보 확인 페이지( )에서 입력하는 비밀번호를 정보통신망을 통하여 송·수신 시 암호화 하지 않았다.

< 해커가 열람한 개인정보가 포함된 페이지 목록 >

구분	URL / 페이지명	포함 개인정보
Mobile	(회원 정보 조회)	이름, 이메일, 휴대전화번호, 생년월일
	(간편결제 리스트)	카드번호 8자리(나머지 8자리 마스킹)
	(상품 페이지)	이름, 휴대전화번호, 배송지 주소
PC	(간편결제 리스트)	카드번호 8자리(나머지 8자리 마스킹)
	(상품 페이지)	이름, 휴대전화번호, 배송지 주소

1) (유출 내용) 이용자 개인정보* 125,138건

* 이름, 휴대전화번호, 생년월일, 배송지 주소, 이메일, 신용카드번호(마스킹)

< 개인정보 세부 유출 항목 및 규모 >

이름, 휴대폰번호, 생년월일, 배송지, 이메일	이름, 휴대폰번호, 생년월일, 배송지, 이메일, 신용카드번호 8자리(나머지 8자리 마스킹)	이름, 휴대폰번호, 생년월일, 배송지, 이메일, 신용카드번호 12자리(나머지 4자리 마스킹)	계 (건)
115,239	9,832	67	125,138

* 피심인은 모바일( )과 PC( )의 카드번호 마스킹 적용 정책이 상이한데, 해커가 67명의 계정으로 모바일과 PC에 모두 접속한 것을 확인하였음. 이 경우, 노출되는 신용카드번호는 임

2) 유출 인지 및 대응

일 시	유출인지 및 대응 내용
’23. 11. 21. 12:30	모바일 서비스 연동 지연 징후가 발생하여, 로그 확인 및 이상 징후 최초 보고
’23. 11. 21. 17:00	자체 점검 결과, 크리덴셜 스터핑 공격 및 개인정보 **유출 인지**
’23. 11. 21. 17:25	모바일 및 PC 페이지 회원정보 수정 페이지 접속 시 및 비밀번호 변경 시 심플 캡챠 적용
‘23. 11. 21. 20:17, 21:57	모바일 및 PC 페이지 ID/PW 로그인 시 심플 캡챠 적용
‘23. 11. 22. 12:00	유출 의심 이용자 계정 비밀번호 초기화 진행
‘23. 11. 22. 16:46	개인정보 포털에 개인정보 **유출 신고**
‘23. 11. 22. 17:30	유출 이용자 대상 계정 초기화 및 PW 변경 안내(문자)
‘23. 11. 23.	비정상적인 로그인 시도에 대한 탐지·차단 보안 정책 적용
‘23. 11. 23. 16:50	개인정보 유출 이용자 대상 **유출 통지**(이메일, 문자)
‘23. 11. 23. 18:30	개인정보 유출 관련 홈페이지, 모바일 팝업 안내
‘24. 2. 16.	회원정보 수정 내 로그인 정보 확인 페이지에 비밀번호 암호화 적용

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ‘17. 12월부터 운영 중인 웹사이트(m.skstoa.com(모바일), skstoa.com(PC))의 회원 로그인 페이지( )에 대해 동일 IP 주소에서 대량의 반복적인 로그인 시도* 등 비정상적인 접근시도를 방지하기 위한 침입 탐지·차단 정책 관리 및 이상행위 대응 등 접근통제 조치를 소홀히 한 사실이 있다.

* 비공격 기간(’23.11.6.~11.13.) 일평균 로그인 시도 건수 : 6,690건
공격 기간(‘23.11.14.~11.21.) 일평균 로그인 시도 건수 : 7,310,304건(약 1,092배)
(동일 IP 주소에서 초당 최대 372회, 평균 92회 로그인 시도)

그 결과, 해커는 ’23. 11. 14. 00:42 ~ 11.21. 23:19 동안 피심인이 운영 중인 웹사이트의 로그인 페이지에 크리덴셜 스터핑 공격을 하여 이용자의 개인정보를 열람하였으며, 피심인은 해커의 공격을 탐지·차단하지 못한 사실이 있다.

한편, 피심인은 회원정보 수정 페이지( )에 보안 통신 프로토콜(HTTPS)이 자동 적용되도록 조치를 하지 않아, 이용자가 데이터 보안이 취약한 HTTP 방식으로 해당 페이지에 접속하여 로그인 정보를 확인할 경우 비밀번호를 평문으로 전송한 사실이 있다.

※ 피심인은 사고 당시 해당 회원정보 수정 페이지 외에는 모두 HTTP로 변환하여 접속할 경우에도 HTTPS가 강제 적용되도록 설정하였음

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 ‘24. 2. 28. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 3. 15. 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[2](이하 ‘시행령’) 제30조제1항제3호는 “개인정보에 대한 접근을 통제하기 위해 ‘개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치(가목)’, ‘개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보

2) 개인정보 보호법 시행령(대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행)

호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단(나목)', '그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)'를 해야 한다"라고 규정하고 있다.

시행령 제30조제1항제4호는 "개인정보를 안전하게 저장·전송하는데 필요한 '비밀번호의 일방향 암호화 저장 등 인증정보의 암호화 저장 또는 이에 상응하는 조치(가목)', '주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장 또는 이에 상응하는 조치(나목)', '「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제1항제1호에 따른 정보통신망을 통하여 정보주체의 개인정보 또는 인증정보를 송신·수신하는 경우 해당 정보의 암호화 또는 이에 상응하는 조치(다목)', '그 밖에 암호화 또는 이에 상응하는 기술을 이용한 보안조치(라목)'를 해야 한다"라고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 「개인정보의 안전성 확보조치 기준[3]」(이하 '안전성 확보조치 기준') 제6조제1항은 "개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한(1호)', '개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응(2호)'의 안전조치를 하여야 한다"라고 규정하고 있다.

안전성 확보조치 기준 제7조제1항은 "개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다."라고 규정하고 있다.

2. 위법성 판단

3) 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 시행)

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인은 '17. 12. 1.부터 운영 중인 웹사이트(m.skstoa.com(모바일), skstoa.com(PC))의 회원 로그인 페이지( )에 대해 동일 IP 주소에서 대량의 반복적인 로그인 시도와 같은 비정상적인 접근시도를 방지하기 위한 침입 탐지·차단 정책 관리 및 이상행위 대응 등 접근통제 조치를 소홀히 한 행위는 보호법 제29조, 시행령 제30조제1항제3호, 안전성 확보조치 기준 제6조제1항을 위반한 것이다.

※ 피심인은 동일 IP 주소에서 대량의 반복적인 로그인 시도를 방지하기 위한 침입 탐지·차단 관련 보안정책은 별도로 적용·운영하지 않았으며, 피심인이 사고 발생 이전 적용한 로그인 "실패" 시 로그인 제한 정책은 크리덴셜 스터핑 공격을 예방할 수 있는 조치라고 볼 수 없음

또한, 피심인이 회원정보 수정 페이지( )에 대해 보안 통신 프로토콜(HTTPS)이 자동 적용되도록 조치를 하지 않아, 이용자가 데이터 보안이 취약한 HTTP 방식으로 해당 페이지에 접속하여 로그인 정보를 확인하는 경우 비밀번호를 평문으로 전송한 행위는 보호법 제29조, 시행령 제30조제1항제4호, 안전성 확보조치 기준 제7조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무	보호법 §29	§30① 제3호	• 개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도 탐지·차단하지 못한 행위 (안전성 확보조치 기준 §6①)
		§30① 제4호	• 비밀번호 등 인증정보를 정보통신망을 통해 송·수신 시 안전한 암호 알고리즘으로 암호화하지 않은 행위 (안전성 확보조치 기준 §7①)

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2제1항

제9호, 시행령 제60조의2 [별표 1의5] 및「개인정보보호 법규 위반에 대한 과징금 부과기준[4]」(이하 '과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제64조의2제1항, 시행령 제60조의2에 따라 위반행위가 있었던 사업연도 직전 3개 사업연도의 연평균 매출액의 100분의 3을 초과하지 아니하는 범위에서 부과할 수 있다.

나. 기준금액

1) 중대성의 판단

과징금 부과기준 제8조제1항은 "시행령 [별표 1의5] 2. 가. 1) 및 2)에 따른 위반행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준을 기준으로 정한다." 라고 규정하고 있다.

[별표] 위반행위의 중대성 판단기준에 따르면 "위반행위의 중대성의 정도는 고려사항별 부과기준을 종합적으로 고려하여 판단'하고, '고려사항별 부과수준 중 두 가지 이상에 해당하는 경우에는 높은 부과수준을 적용한다.'라고 규정하고 있으며, '고려사항별 부과수준의 판단기준은 ▲(고의 · 과실) 위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려, ▲(위반행위의 방법) 안전성 확보 조치 이행 노력 여부, 개인정보 보호책임자 등 개인정보 보호 조직, 위반행위가 내부에서 조직적으로 이루어졌는지 여부, 사업주, 대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 개인정보의 유출등과 안전성 확보 조치 위반행위와의 관련성을 포함하여 판단, ▲(위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향) 피해 개인정보의 규모, 위반기간, 정보주체의 권리 · 이익이나 사생활 등에 미치는 영향 등을 종합

4) 개인정보보호 법규 위반에 대한 과징금 부과기준(개인정보보호위원회 고시 제2023-3호, 2023. 9. 15. 시행)

적으로 고려하고, 개인정보가 유출등이 된 경우에는 유출등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.”라고 규정하고 있다.

피심인의 고의·과실, 위반행위의 방법, 처리하는 개인정보의 유형, 정보주체의 피해 규모 및 정보주체에게 미치는 영향 등을 종합적으로 고려하여, 위반행위의 중대성을 ’보통 위반행위‘로 판단한다.

3) 기준금액 산출

과징금 부과기준 제6조제1항은 ‘기준금액은 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액에 부과기준율을 곱한 금액으로 정한다’라고 규정하고 있다.

피심인의 경우, 과징금 부과기준 제7조제3항에 따라 위반행위와 관련이 없는 매출액은 피심인의 매출액과 매출액 중 관련 매출액인 천 원으로 하고, 직전 3개 사업년도의 연평균 전체 매출액에서 관련 없는 매출액을 제외한 천 원에 시행령 [별표 1의5] 2. 가. 1)에 따른 ‘보통 위반행위’의 부과기준율 1천분의 12를 적용하여 기준금액을 천 원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천 원)

구 분	2020년	2021년	2022년	평 균
①전체 매출액				
②관련 없는 매출액				
①에서 ②를 제외한 매출액				

※ 피심인이 제출한 회계자료를 토대로 작성

<시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	2.1% 이상 2.7% 이하
중대한 위반행위	1.5% 이상 2.1% 미만
보통 위반행위	**0.9% 이상 1.5% 미만**
약한 위반행위	0.03% 이상 0.9% 미만

다. 1차 조정

과징금 부과기준 제9조에 따라 피심인 위반행위의 기간이 2년을 초과('17. 12. 1. ~ '23. 11. 23.)하여 '장기 위반행위'에 해당하므로 기준금액의 100분의 50에 해당하는 금액인 천 원을 가산하고,

위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우에 해당하여 기준금액의 100분의 30에 해당하는 금액인 천 원을 감경한다.

라. 2차 조정

과징금 부과기준 제10조에 따라 피심인이 ▲과징금의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우, ▲조사에 적극 협력한 경우, ▲개인정보 보호를 위해 보호위원회가 인정하는 인증을 받은 경우에 해당하여 1차 조정을 거친 금액의 100분의 50에 해당하는 천 원을 감경한다.

마. 부과과징금의 결정

과징금 부과기준 제11조제1항은 ▲위반행위자의 현실적인 부담 능력, ▲위반행위자가 속한 시장·산업 여건 등(1. 위반행위자의 자산, 자기자본 등 재무상황에 비추어 위반행위자가 과징금을 부담할 능력이 현저히 부족하다고 객관적으로 인정되는 경우, 2. 경제위기 등으로 위반행위자가 속한 시장·산업 여건이 현저하게 변동되거나 지속적으로 악화된 상태인 경우)을 고려하여 제10조에 따라 산정된 과징금이 과중하다고 인정되는 경우에는 해당 금액의 100분의 90 범위에서 감경할 수 있다고 규정하고 있다.

위원회는 디지털 전환에 따른 온라인 시장 확장, TV시청 인구·시청률 감소, 송출 수수료 증가 등으로 피심인이 속한 TV 및 데이터 홈쇼핑 업계의 시장·산업 여건이 지속적으로 악화되고 있는 점 등을 종합적으로 고려하여 과징금 부과기준 제11조제1항에 따라 1차 조정, 2차 조정을 거친 금액의 100분의 30에 해당하는 천 원을 감경한다.

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제64조의2 제1항제9호, 시행령 제60조의2, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 천 원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④부과과징금 결정	⑤최종과징금
•직전 3개 사업연도 연평균 매출액 (천 원*) •연평균 매출액에 1.2% 적용 (보통 위반**)	•위반기간*** 2년 초과 50% 가중 (천 원) •취득이익 없으므로 30% 감경 (천 원)	•시정완료, 조사협력, ISMS-P 인증으로 50% 감경 (천 원)	•위반행위자가 속한 업계의 시장·산업 여건 등을 종합적으로 고려하여 30% 감경 (천 원)	**천 원****

* 전체 매출액에서 위반행위와 관련 없는 매출액(매출액, 매출액 중 관련 매출액)은 제외함

** ①(고의·과실:중) ▲고의성 없음, ▲중과실, ▲위반행위로 인한 영리 목적 없음, ▲자체 모니터링으로 해킹 공격 및 유출 인지 등 적극 대응 노력 등(참작)

②(부당성:하) ▲안전조치의무 1개 조항 관련이나, ▲ISMS-P 인증, 방화벽·웹방화벽·IPS 등 보안 시스템 도입, 로그인 실패 시 계정 잠금 등 보안정책 적용, ▲개인정보보호 책임자 및 조직 구성, ▲조직적인 행위 미해당, ▲대표자 또는 임원의 책임·관여 미해당

③(개인정보 유형:하) ▲고유식별정보, 민감정보, 인증정보 미해당

④(피해규모:중) ▲유출 규모 약 12만 건, ▲위반 기간 : '17.12.1.~'23.11.23.(5~6년) ▲공중 미노출, ▲이름, 휴대전화번호, 생년월일, 주소 등 유출로 피해 영향도가 낮다고 볼 수 없음

*** 위반기간 : '17. 12. 1. ~ '23. 11. 23.

**** 과징금 부과기준 제11조제5항에 따라 부과과징금이 1억원 이상인 경우에는 1백만 원 단위 미만의 금액을 버림

2. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 위반행위 중 개인정보의 암호화 미조치 행위(안전성 확보조치 기준 제7조제1항)에 대한 과태료는 같은 법 제75조(과태료)제2항 제5호, 시행령 제63조 [별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[5] (이하 '과태료 부과기준')에 따라 다음과 같이 부과한다.

※ 보호법 제29조 위반행위 중 시행령 제30조제1항제3호(안전성 확보조치 기준 제6조제1항) 위반행위의 경우, 과징금을 부과한 행위이므로 보호법 제76조에 따라 과태료를 부과하지 않음

가. 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 제29조(안전조치의무) 위반에 대해서는 1회 위반에 해당하는 과태료인 600만 원을 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 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**	법 제75조 제2항제5호	600	1,200	2,400

5) 개인정보 보호법 위반에 대한 과태료 부과기준(개인정보보호위원회 지침, 2023. 9. 15. 시행)

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과기준 제8조는 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표3]의 가중기준(▲위반의 정도, ▲위반기간, ▲조사방해, ▲위반주도 등을 고려하여 가중사유가 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 보호법 제29조(안전조치의무) 위반행위에 대하여 과태료 부과기준 제8조에 따라 특별히 가중할 사유는 없다.

※ 보호법 제29조 위반행위 중 시행령 제30조제1항제3호(안전성 확보조치 기준 제6조제1항) 위반행위의 경우, 과징금을 부과한 행위이므로 보호법 제76조에 따라 과태료를 부과하지 않음

2) (과태료의 감경) 과태료 부과기준 제7조는 '당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준(▲당사자 환경, ▲위반정도, ▲개인정보보호 노력정도, ▲조사협조 및 자진시정 등을 고려하여 감경사유가 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 보호법 제29조(안전조치의무) 위반행위에 대하여 ▲위반행위자가 법 제32조의2에 따른 개인정보 보호 인증(ISMS-P)을 받은 경우, ▲보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우, ▲과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우 등을 종합적으로 고려하여 과태료 부과기준 제7조에 따라 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 300만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무	600만 원	-	300만 원	**300만 원**
계				**300만 원**

3. 결과 공표명령

보호법 제66조제2항 및 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침[6]」(이하 '공표 및 공표명령 지침') 제6조제1항에 따라 '위반행위 시점을 기준으로 위반 상태가 3년을 초과하여 지속된 경우(7호)', '위반행위로 인하여 피해를 입은 정보주체의 수가 10만 명 이상인 경우(8호)'에 해당하고 위반행위가 인터넷을 통하여 이루어졌으므로 제8조 및 제11조에 따라 처분등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분등을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 6분의1 크기로 2일 이상 5일 미만의 기간 동안(휴업일 포함) 공표하도록 명한다. 다만, '1일간 다시 보지 않기' 기능의 사용 등 팝업창 설정방식 등은 보호위원회와 협의하여 정한다.

이때 제7조제1항, 제8조제3항에 따라 원칙적으로 공표지침 [별표]의 표준 공표문안을 따르되, 공표 문안 등에 관하여 보호위원회와 미리 문서로 협의해야 하고, 제11조제3항에 따라 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 보호위원회와 협의하여 정한다.

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2(과징금의 부과)제1항제9호, 시행령 제60조의2(과징금의 산정기준 등), 제75조(과태료) 제2항제5호, 제76조(과태료에 관한 규정 적용의 특례), 제66조(결과의 공표)에 따라 과징금, 과태료, 결과의 공표명령을 주문과 같이 의결한다.

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

이의제기 방법 및 기간

피심인은 이 과징금 부과처분, 공표명령에 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.

2025년 1월 22일

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)