개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2023-004-034호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2023. 3. 8.

주 문

1. 피심인 에 대하여 다음과 같이 과징금과 과태료를 부과한다.

   가. 과 징 금 : 원

   나. 과 태 료 : 7,200,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

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

이 유

Ⅰ. 기초 사실

온라인 쇼핑몰을 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('22. 9. 22.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('22. 10. 12. ~ '23. 2. 8.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 온라인 쇼핑몰( )를 운영하면서 '22. 10. 24. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보	(필수) (선택)	~ 계속	
합 계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

피심인은 '22. 9. 21. 온라인 쇼핑몰에서 결제 오류가 발생한다는 민원을 받고 시스템을 점검한 결과 '22. 9. 22. 오전 페이지 변조 사실 등을 확인하고 '22. 9. 22. 개인정보 유출을 신고하는 등 아래와 같이 3회의 유출 신고와 6회의 유출 통지를 실시한 바 있다.

구분	인지 시점	유출 신고·통지 시점
1 (신고)	**'22. 9. 22. 오전** 페이지 변조 사실, 기능 등을 확인	**'22. 9. 22. 17:16** 1차 유출신고 -결제정보
2 (통지)	**'22. 9. 22.** 로그를 확인 후 유출 대상자 확인	**'22. 9. 23. 10:52** 1차 유출통지(20명) -결제정보
3 (신고)	**22. 10. 14. 17시경** KISA로부터 긴급 대응 메일을 수신하고 회원정보임을 확인 ※ 피심인은 '22.9.22. KISA에 기술지원 신청	**'22. 10. 18. 16:13** 2차 유출신고 -회원정보
4 (통지)		**'22. 10. 19. 12:40** 2차 유출통지(명) -회원정보*
5 (통지)	**'22. 10. 20.** 결제 미종료 이용자 20명 추가 확인	**'22. 10. 21. 15:03** 3차 유출통지(20명) -결제정보
6 (신고)	**'22. 10. 26. 17:30** 로그분석 중 주문정보 3건 유출 인지	**'22. 10. 26. 17:43** 3차 유출신고 –주문정보
7 (통지)		**'22. 10. 27. 14:00** 4차 유출통지(3명) -주문정보
8 (통지)	**'22. 11. 10.** IP를 분석 결과, 결제정보가 유출된 기존 40명 외에 35명의 결제정보 추가 유출 확인 ※ '22. 11. 9. 위원회가 추가유출 가능성 안내	**'22. 11. 10. 14:00** 5차 유출통지(27명) -결제정보
9 (통지)		**'22. 11. 11. 15:00** 6차 유출통지(8명) -결제정보

2) 유출규모 및 경위

(유출항목 및 규모) 명의 개인정보(중복 유출된 정보주체 수 제외)

- 명의 회원정보(ID, 이름, 주소, 생년월일 등)와 명의 주문정보(이름, 주소, 휴대전화번호) 및 명의 결제정보(카드번호, 유효기간 등)

구분	유출항목	확인된 내용
회원정보 (명)	회원번호, 아이디, 비밀번호(암호화), 이름, 별명, 이메일(암호화), 휴대전화번호(암호화), 주소, 성별, 생년월일, IP, APIKey(암호화)	다운로드(dump)된 테이블은 라 인이며, 삭제된 데이터 제외 시 명 의 회원정보 유출 확인(피심인 분석결과)
주문정보 (명)	이름, 주소, 휴대전화번호	조회(Select)된 테이블은 라인이며, 명의 주문정보 유출 확인(피심인 분석결과)
결제정보 (명)	카드번호, 유효기간, CVC, 주민등록번호, 신용카드 비밀번호, 일반결제 비밀번호, 휴대전화번호	변조된 결제 페이지의 기능상 결제정보의 외부전송 사실 확인(위원회 분석결과) 및 명의 결제정보 유출(피심인 분석결과)

※ 피심인은 결제정보를 자체 수집하지 않고 PG사(KCP, 토스) 결제 서비스를 이용하나, 해커가 변조 페이지를 이용하여 카드번호 등 결제정보를 수집·유출한 것임

(유출경위) 해커가 온라인 쇼핑몰 문의 게시판에 악성코드 파일(test.php, mysql.php)을 업로드·실행하는 웹셸공격을 통해 개인정보처리시스템에 접속하여, 회원정보와 주문정보를 조회·다운로드하고, 결제정보를 외부 전송하여 이용자 개인정보가 유출됨

일시	해커의 행위
알 수 없음	공동구매·특판·수출 문의 게시판(www. .co.kr/board/?id=propose_bbs)에 악성코드 파일을 업로드한 것으로 추정
'22.9.16. 20:17	m. . .kr 도메인을 이용하여 웹서버에 접속, 공동구매·특판·수출 문의 게시판에 업로드된 악성코드(test.php, mysql.php)를 실행
'22.9.16. 20:20	DB 관리 프로그램(mysql.php)을 이용하여 DB에 접속
'22.9.16. 20:24	**fm_member 테이블(명의 회원정보)**을 다운로드(dump)하고 **fm_order 테이블(명의 주문정보)**을 조회(select)함으로써 회원정보와 주문정보를 유출
'22.9.16-17.	로그인 후 변조된 결제 모듈 테스트 진행 및 결제 페이지 변조
'22.9.22.-23.(추정)	**명의 결제정보**를 외부 도메인( )으로 전송하여 유출

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 방화벽, 웹방화벽, 침입방지시스템을 설치하였으나, '19. 7. 19.부터 관리용 도메인( ) 또는 웹서버 IP 주소( )로 접속하는 트래픽의 경우 웹방화벽을 거치지 않고 개인정보처리시스템에 접속할 수 있게 하고, 방화벽과 침입방지시스템이 접근제한 및 유출탐지 기능을 충족하도록 운영하지 않았으며, php 파일이 업로드되어 실행되도록 하는 등 접근통제를 소홀히 하여 이용자 명의 개인정보가 유출되도록 한 사실이 있다.

< 피심인의 네트워크 구성 현황('19. 7. ~ '23. 1.)>

① 방화벽 : 서비스 운영에 필요한 포트를 오픈하는 용도로 사용하였을 뿐 접근제한 및 유출탐지 기능이 실행되도록 운영하지 않음

② 웹방화벽 : 공격으로 판단되는 IP를 차단하나, 관리용 도메인( )이나 웹서버 IP 주소( )로 접속 시 웹방화벽을 거치지 않고 우회토록 네트워크 구성

③ 침입방지시스템 : https로 암호화된 트래픽을 탐지·차단할 수 있는 인증서를 설치하지 않아 암호화되어 송수신되는 유해 트래픽을 탐지할 수 없게 됨으로써 해커의 접속 도메인(https://)이 탐지되지 않는 등 접근제한 또는 유출 탐지 기능이 수행되도록 운영하지 않음

나. 개인정보 유출 통지를 소홀히 한 행위

피심인은 ’22. 10. 14. 17시경 한국인터넷진흥원으로부터 개인정보가 저장된 DB 테이블이 유출되었고, 개인정보 유출 등을 신고 및 통지할 것을 안내하는 내용의 ‘중소기업 피해지원 긴급 대응 방안 안내’ 메일을 수신하고 회원정보임을 확인하는 등 유출을 인지하였음에도, 추가 유출이 확인된 회원정보에 대하여 ‘22. 10. 18. 16:13에 이르러서야 유출을 신고하고, ’22. 10. 19. 12:40 회원들에게 유출을 통지하는 등 정당한 사유 없이 24시간을 경과하여 신고·통지를 지연한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’23. 2. 9. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’22. 2. 24. 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 “개인정보처리시스템에 대한 침입차단 시스템 및 침입탐지시스템의 설치·운영(나목)”, “그 밖에 개인정보에 대한 접근

통제를 위하여 필요한 조치(마목)' 등의 조치를 하여야 한다."라고 규정하고 있다.

같은 법 시행령 제48조의2제3항은 "제1항에 따른 안전성 확보 조치에 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 제2020-5호, 이하 '고시') 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있으며

고시 제4조제9항은 "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.

나. 보호법 제39조의4제1항은 "정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 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 조

치를 취할 수 있다.”라고 규정하고 있다.

같은 법 시행령 제48조의4제2항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면등의 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

[보호법 제29조(안전조치의무)]

피심인이 개인정보처리시스템에 대한 접근제한 및 유출탐지, 웹셸 업로드 및 실행 제한 등의 접근통제를 소홀히 하여 개인정보가 유출되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항 및 제9항을 위반한 것이다.

나. 개인정보 유출 통지를 소홀히 한 행위

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

피심인이 ‘22. 10. 14. 한국인터넷진흥원을 통해 개인정보 유출 및 신고·통지를 안내받고 회원정보임을 확인하였음에도 유출 사실을 안 때부터 정당한 사유 없이 24시간을 경과하여 ‘22. 10. 18.과 ’22. 10. 19.에 각 신고 및 통지한 행위는 보호법 제39조의4, 시행령 제48조의4를 위반한 것이다.

이와 관련하여, 피심인은 ’22. 10. 14. 금요일 17시경 한국인터넷진흥원으로부터 개인정보 유출 가능성에 대한 안내 메일을 수신하였고, 해당 메일의 근거자료가 웹 서버 접속 로그 2줄에 불과하므로 유출 항목과 대상자 파악이 곤란하여 곧바로 신고·통지를 할 수 없었으며, ‘22. 10. 18. 17시경 최종 회원정보 유출을 인지하고 24시간 내에 신고(’22. 10. 18. 16:13) 및 통지(‘22. 10. 19. 12:40)한 것이므로 정당한 사유 없이 신고·통지를 지연한 사실이 없다고 주장한다.

그러나 피심인은 ’22. 9. 22. 1차 신고·통지를 하면서 해커의 공격으로 20여 건의 결제정보가 유출되었다는 사실을 파악하고 있었고, ‘22. 10. 14. 한국인터넷진흥원이 피심인에게 송부한 이메일에는 웹 서버 접속 로그뿐만 아니라 ’개인정보가 유출된 것으로 확인됩니다’, ‘공격자에 의해 유출된 정보는 데이터베이스 내 ’fm_member‘ 테이블로 확인됩니다’라는 표현이 기재되어 있었으며, 피심인은 데이터베이스의 fm_member 테이블에 회원 이용자의 이름, 주소, 생년월일, 휴대전화번호 등의 정보를 보관하고 있었으므로 해당 이메일을 수신한 시점에 회원정보의 유출 사실을 즉시 인지하였다고 보아야 한다.

한편, 현행 보호법은 정보통신서비스 제공자등에 대해 개인정보 유출등 발생 시 파급력과 전파력을 고려하여 개인정보처리자의 통지 시한인 5일보다 단기의 기간인 24시간을 법률에서 명확하게 규정하고 있고, 같은 법 시행령 제48조의4제3항에서 유출된 개인정보 항목과 유출 발생 시점에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 이용자가 취할 수 있는 조치 등의 사항을 우선 통지·신고한 후 추가 확인되는 내용에 대해서 확인되는 즉시 통지·신고하도록 규정하고 있으며, ’개인정보 보호 법령 지침·고시 해설‘ 354면은 ’인지 시점‘에 대하여, 개인정보처리자가 유출사실을 확신할 것까지 요하지는 않고 개인정보처리자의 관리·통제권을 벗어나 제3자가 개인정보를 알 수 있는 상태에 이르렀다는 사실을 알게 되었을 때에 유출사실을 안 때에 해당한다고 기술하고 있다.

이 같은 보호법 규정의 취지와 시행령 규정 및 관련 해설의 내용에 따라, 정보통신서비스제공자등은 유출항목과 유출 발생 시점 등이 확인되지 않았으면 그때까지 확인된 내용 등을 우선 신고·통지하여야 하나 피심인은 4일 이상 경과할 때까지 일부 항목에 대해서도 신고·통지를 하지 않았고, 피심인의 데이터베이스 내 fm_member 테이블에 회원 이용자의 이름, 주소, 생년월일, 휴대전화번호 등의 회원정보가 보관되고 있었던 점을 고려하면 유출항목 및 통지 대상을 파악하는 것에 4일의 시간이 소요된다고 보기도 어려워 신고·통지 지연에 정당한 사유가 있다고 할 수도 없는바, 피심인의 주장을 받아들일 수 없다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§48의2① 제2호	• 개인정보처리시스템에 대한 접근제한 및 유출탐지 등 정보통신망을 통한 불법적인 접근 및 침해사고 방지 시스템 운영을 소홀히 한 행위(고시§4⑤) • 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 소홀히 한 행위(고시§4⑨)
개인정보 유출등의 통지·신고에 대한 특례 위반	보호법 §39의4①	§48조의4	• 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 유출신고·통지한 행위

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(이하 '과징금 부과기준'이라 한다)'에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29항 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 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.

피심인은 영리를 목적으로 정보통신망을 통해 정보통신서비스를 제공하는 자이고, 2년을 초과하여 보호법 제29조의 접근통제 등 안전조치의무를 소홀히 하였으므로 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 3개에 해당하는 경우 '보통 위반

행위’로, 1~2개에 해당하는 경우 ‘중대한 위반행위’로 감경하도록 규정하고 있다.

피심인의 경우 위반행위로 인해 직접적으로 이득을 취하지 않은 경우, 이용자의 개인정보가 공중에 노출되지 않은 경우에 해당하여 ‘중대한 위반행위’로 감경한다.

3) 기준금액 산출

피심인의 온라인 쇼핑몰(.co.kr)을 통해 발생한 매출을 위반행위 관련 매출로 하고, 직전 3개 사업년도의 연평균 매출액 천원에 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 ‘중대한 위반행위’의 부과기준율 1천분의 21을 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2019년	2020년	2021년	평 균
관련 매출액*				

* 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

<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 피심인 위반행위의 기간이 2년을 초과

하여 ‘장기 위반행위’에 해당하므로 기준금액의 100분의 50을 가중하고,

최근 3년 이내 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50을 감경하여 기준금액을 유지한다.

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.

피심인이 ▲조사에 적극 협력한 점, ▲개인정보 유출사실을 자진 신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 천원을 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 천원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금
천원	① 기준금액의 50% 가중 (장기위반 : 천원) ② 기준금액의 50% 감경 (최초위반 : 천원)	① 추가적 가중없음 ② 추가적 감경 (20%, 천원)	천원
	→ 천원	→ 천원	

한편, 과징금 부과기준 제9조제1항은 위반행위자의 자산, 자기자본 등 재무상황에 비추어 과징금을 부담할 능력이 현저히 부족하다고 객관적으로 인정되는 경우(제1호), 개인정보 분쟁조정, 민사조정 등을 통해 정보주체에게 발생한 피해에 대한 원상회복, 손해배상 또는 이에 상당하는 필요한 구제조치를 한 경우(제2호), 경제위기 등으로 위반행위자가 속한 시장·산업 여건이 현저하게 변동되거나 지속적으로 악화된 상태인 경우(제3호) 과징금 부과기준 제8조에 따라 산정된 과징금 해당 금액의 100분의 90 범위에서 감경할 수 있다고 규정하고 있다.

이와 관련하여, 피심인은 '22년 추정 영업이익이 '20년 대비 % 감소하고 당기순손실이 예상되는 등 경영상의 어려움이 지속되어 %의 감축을 진행하였으며, 시장 전망이 악화되고 있고, 본 건과 관련하여 신용카드 결제 피해가 발생하였다고 주장하는 2명의 이용자를 대상으로 원의 배상을 진행하였으며, '21년부터 개인정보보호배상책임보험에 가입하여 피해구제 관련 선제적 조치를 진행하고 있는 점 등을 고려하여 과징금의 감경을 요청하였다.

그러나 피심인의 '21년까지의 당기순이익을 고려하면('19.~'21. 3년 평균 억) 현실적 과징금 부담 능력이 현저히 부족하다고 보기 어렵고, 위반행위자가 속한 시장·산업 현황과 관련하여 특별한 과징금 감경 사유를 인정하기도 어렵다. 나아가, 피심인은 보호법 제39조의9에 따라 개인정보보호배상책임보험 등에 가입할 의무가 있는 자로, 보험에 가입한 사실과 유출대상 명(결제정보 유출 명) 중 2명에게 배상하였다는 사정만으로 정보주체의 피해에 대한 원상회복, 손해배상 또는 이에 상당하는 필요한 구제조치를 하였다고 인정하기 어려운바, 최종 산정된 과징금을 유지하기로 한다.

2. 과태료 부과

피심인의 보호법 제29조(안전조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제12호의3, 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 각 위반행위별 기준 금액을 600만원으로 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
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

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, 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위는 '법 위반상태의 기간이 3개월 이상인 경우'에 해당하므로 기준금액의 10%를 가중하고, 개인정보 유출 신고 및 통지를 소홀히 한 행위는 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개인 경우'에 해당하여 기준금액의 10%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, 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위와 개인정보 유출 신고 및 통지를 소홀히 한 행위 모두 '과태료의 사전통지 및 의견 제출 기간 내에 법규 위반행위를 중지하는 등 시정을 완료한 경우'와 '조사에 적극 협력한 경우' 등에 해당하여 기준금액의 50%를 각 감경한다.

다. 최종 과태료

피심인의 보호법 제29조 및 제39조의4제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 720만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만원	60만원	300만원	**360만원**
개인정보 유출등의 통지·신고에 대한 특례	600만원	60만원	300만원	**360만원**
계				**720만원**

3. 결과 공표

보호법 제66조제1항 및 '개인정보보호위원회 처분결과 공표기준'(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 '법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우'(제4호), '위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우'(제5호), '개인정보 유출 및 침해사고로 인한 피해자 수가 10만 명 이상인 경우'(제7호)에 해당하므로 피심인에 대한 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표				
위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	위반조항	위반내용	처분일자	처분내용
	법 제29조	안전조치의무 위반	2023.3.8.	과태료 부과 360만원
	법 제39조의4제1항	유출 통지·신고에 대한 특례 위반	2023.3.8.	과태료 부과 360만원

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대하여 같은 법 제39조의15(과징금의 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항제6호·제12호의3, 제66조(결과의 공표)제1항에 따라 과징금·과태료 부과 및 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 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.

2023년 3월 8일

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 흥 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)