개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2022-013-103호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2022. 8. 10.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

2) 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하거나 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 등 침입차단·탐지시스템을 운영하여야 한다.

3) 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

나. 피심인은 개인정보의 유출 사실을 인지한 때로부터 24시간 이내에 유출 사실을 통지·신고하여야 하고, 유출 사실에 대한 이용자 통지 시 법정 통지 항목을 모두 포함하여 통지하여야 한다.

다. 피심인은 가.와 나.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 원

나. 과 태 료 : 14,400,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

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

이 유

Ⅰ. 기초 사실

피심인은 영리를 목적으로 웹( )·앱 온라인 쇼핑몰 서비스를 제공하는 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16955호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 온라인쇼핑몰 운영 중 신원미상자(이하, '해커')의 접근통제가 되지 않아 이용자의 개인정보가 유출되었다고 신고('22. 3. 16., '22. 4. 8.)하였고, 이용자가 로그인 시 다른 이용자의 로그인 정보가 노출되었다고 신고함('22. 5. 17.)에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('22. 3. 22. ~ 6. 3.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 온라인쇼핑몰을 운영하면서 ’22. 3. 30. 기준 1,795,304건의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보	이름, 주소, 휴대전화번호, 비밀번호, 이메일, 성별, 아이디, 결제정보, 생년월일 등	‘16. 1. 29. ~ 계속	(유효) 1,574,005 (분리) 221,299
계			1,795,304

나. 개인정보 유출 경위

< ① 개인정보 유출 사건(’22. 3. 16일, ’22. 4. 8일 유출 신고건) >

1) 유출 경과 및 대응

일 시	피심인의 유출인지 및 대응 내용
’22. 3. 14. 11:52	로부터 보안 이슈 관련 메일 수신
’22. 3. 16. 15:10	DB 로그 분석 과정에서 회원 테이블 조회 사실인지
’22. 3. 16. 21:19	개인정보보호 포털에 개인정보 유출신고(KISA, 1차)
’22. 3. 17. 15:00	홈페이지 유출 사실 공지 및 이용자 대상 이메일 통지(1,536,399건)
’22. 3. 17. ~	IP 차단조치 실행 및 유출에 악용된 관리자계정( )과 웹셸 삭제
’22. 4. 8. 10:03	로부터 보안 이슈 관련 메일 재수신
’22. 4. 8. 11:30	DB로그 분석 결과 개인정보 추가 유출 사실인지
’22. 4. 8. 16:30	개인정보 추가 유출 사실 신고(KISA, 2차)
’22. 4. 9. 01:50	홈페이지 유출 사실 공지 및 이용자 대상 이메일 통지(1,629,792건)

2) 유출규모 및 경위

(유출항목 및 규모) 온라인쇼핑몰에 가입한 이용자의 개인정보(이름, 주소, 이메일, 휴대전화번호, 비밀번호, 성별, 아이디, 결제정보, 생년월일 등) 1,536,399건('22. 3. 16. 유출 신고), 1,629,792건('22. 4. 8. 유출신고)

(유출경위) 해커는 웹 취약점, 접근통제 미흡을 이용해 DB에 무단 접근하여 개인정보를 조회·유출

- '16. 1. 29. : 피심인이 온라인 쇼핑몰 서비스 운영을 시작
- '22. 3. 10. 10:02 : 해커가 알 수 없는 방법으로 취득한 관리자계정 ( )으로 관리자페이지에 로그인 성공
- '22. 3. 10. 10:24 : 해커가 관리자페이지에 원격접속이 가능한 웹셸코드 삽입
- '22. 3. 10. 11:25 : 해커가 DB관리도구 설치
- '22. 3. 10. 11:32 : 해커가 DB관리도구의 내보내기(export)기능으로 개인정보 유출(515MB)
- '22. 3. 14. 1:05 : 해커가웹셸 파일을 통해 개인정보 유출(1.5GB)
- '22. 4. 7. 20:29 : 해커가 웹셸 파일을 통해 개인정보 유출(1.6GB)

< ② 개인정보 유출 사건('22. 5. 17일 유출 신고건) >

1) 유출 경과 및 대응

일 시	피심인의 유출인지 및 대응 내용
'22. 4. 29.	타 이용자 정보 노출 관련 최초 민원 접수
'22. 5. 2. 17:16	타 이용자 정보 노출 관련 추가 민원 접수
'22. 5. 2.	계정 토큰 처리 관련 오류 가능성 인지
'22. 5. 6. ~ 5. 11.	토큰 처리시스템 오류수정 및 식별정보 발급 절차 개선
'22. 5. 17.	개인정보보호 포털에 개인정보 유출신고(KISA)
'22. 5. 18.	개인정보 유출 이용자 대상 유선 통지

2) 유출규모 및 경위

(유출항목 및 규모) 이용자의 개인정보 2건*

* 1건(이메일, 주소, 휴대전화번호, 생년월일), 1건(이메일, 주소, 휴대전화번호)

(유출경위) 피심인은 '20. 4. 30.부터 소셜로그인 기능을 제공하면서 이용자 식별정보 추출 오류로 이용자 식별정보(토큰 정보)가 중복되는 문제 발생

3. 개인정보의 취급.운영 관련 사실관계

< ① 개인정보 유출 사건('22. 3. 16일, '22. 4. 8일 유출 신고건) >

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 관리자 계정에 대해 접근권한을 변경말소 조치하여야 하나, 미사용 중인 관리자 계정이 악용되어 개인정보가 유출된 사실이 있다.

또한 피심인은 이용자의 개인정보를 조회·삭제할 수 있는 관리자페이지를 운영

하면서 불법적인 접근을 방지하기 위한 침입 차단·탐지시스템을 설치·운영하는 등 안전조치를 하여야 하나,

개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하거나 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하기 위한 침입 차단·탐지시스템 운영을 소홀히 하여 개인정보가 유출된 사실이 있다.

나. 개인정보 유출통지를 소홀히 한 행위

피심인은 유출 사실에 대한 이용자 통지 시 법정 통지항목을 모두 포함하여 통지하여야 하나, '22. 4. 7. 추가 유출과 관련하여 ①유출된 개인정보 항목과 ②유출이 발생한 시점을 누락하여 통지한 사실이 있다.

< ② 개인정보 유출 사건('22. 5. 17일 유출 신고건) >

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 처리 중인 개인정보가 열람 권한이 없는 자에게 노출되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 하나, 소셜로그인 연동 시 이용자 식별정보 추출 오류로 개인정보가 열람 권한 없는 자에게 노출된 사실이 있다.

나. 개인정보 유출통지를 소홀히 한 행위

피심인은 개인정보 유출 사실을 인지한 때로부터 24시간 이내에 유출 사실을 통지·신고하여야 하나, 정당한 사유 없이 24시간을 초과하여 통지·신고한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022. 6. 3. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 7. 1. 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.

보호법 시행령 제48조의2제1항 제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위해 ‘개인정보를 처리할 수 있도록 체계적으로 구성한 개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(가목)’, ‘개인정보에 대한 불법적인 접근을 차단하기 위하여 침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2020-5호, 이하 ‘고시’) 제4조제2항은 “정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.”라고 규정하고 있고, 고시 제4조제5항은 “정보통신서비스 제공자 등은 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 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

나. 보호법 제39조의4제1항은 “정보통신서비스제공자는 개인정보의 분실·도난·유출 사실을 안 때에는 지체없이 유출 등이 된 개인정보 항목(제1호), 유출 등이 발생한 시점(제2호) 등을 포함한 각 호의 사항을 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.”라고 규정하고 있다.

보호법 시행령 제48조의4제2항은 “정보통신서비스 제공자 등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체없이 법 제39조의4제1항 각 호의 모든 사항을 서면 등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.”라고 규정하고 있다.

2. 위법성 판단

< ① 개인정보 유출 사건('22. 3. 16일, '22. 4. 8일 유출 신고건) >

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 불법적인 접근 차단}

피심인은 국내 대표적인 사업자로 2021년 매출액이 억 원이고, 2022년 3월 기준 개인정보를 보관하고 있는 건수가 179만명 이상으로 일정규모 이상의 사업자에 해당하며, 피심인이 수집한 이름, 생년월일, 휴대전화번호 등의

개인정보는 이용자를 특정할 수 있는 기본적인 개인정보로서 제3자가 이용할 경우 이용자에게 적지 않은 피해가 발생할 수 있어 보안을 철저히 할 필요가 있다.

또한 관리자 계정에 대한 접근권한 변경·말소 조치, 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한, 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도 탐지 등 침입 차단·탐지시스템 운영을 통해 해킹을 방지하는 것은 누구나 생각할 수 있는 보편적으로 알려진 정보보안 기술 수준이고, 사회통념상 합리적으로 기대 가능한 정도의 보호조치에 해당한다.

1) (접근권한 변경·말소) 피심인이 관리자 계정에 대해 접근권한을 변경·말소 조치하지 않고 미사용 중인 관리자 계정을 방치하여 개인정보가 유출되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제2항을 위반한 것이다.

2) (침입 차단·탐지시스템 운영) 피심인이 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는 등 조치를 하지 않고, 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 등 침입 차단·탐지시스템 운영을 소홀히 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항을 위반한 것이다.

나. 개인정보 유출 등의 통지·신고 조치를 하지 않은 행위

{보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)}

피심인은 개인정보의 분실·도난·유출 사실을 안 때에는 지체없이 유출 등이 된 개인정보 항목, 유출 등이 발생한 시점 등을 포함한 법정통지 항목을 모두 포함하여 이용자에게 유출통지 하여야 하나, ’22. 4. 7. 추가 유출 시 유출된 개인정보 항목과 유출이 발생한 시점을 누락하여 통지한 행위는 보호법 제39조의4제1항, 같은 법 시행령 제48조의4제2항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	보호법 §29	§48의2① 제2호	• 관리자페이지에 접속 가능한 계정에 대해 접근권한을 변경·말소하지 않은 행위(고시§4②) • 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하는 등의 접근제한을 하지 않은 행위(고시§4⑤) • 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 등 침입 차단·탐지시스템 운영을 소홀히 한 행위(고시§4⑤)
개인정보 유출통지 위반	보호법 §39의4①	§48의4③	• 이용자에게 유출 사실 통지 시 항목을 누락하여 통지한 행위

< ② 개인정보 유출 사건('22. 5. 17일 유출 신고건) >

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 열람 권한 없는 자에 대한 접근통제}

(개인정보 유·노출 방지) 피심인이 처리중인 개인정보가 열람 권한이 없는 자에게 노출되거나 외부에 유출되지 않도록 개인정보처리시스템에 접근통제 등 보호조치를 취하지 않아 '20. 4. 30.부터 제공한 소셜로그인 연동 기능과 관련하여 이용자 식별정보 추출 오류가 발생하였고, 이에 따라 이용자 식별정보(토큰 정보)가 중복되는 문제가 발생하여 열람 권한 없는 자에게 이용자의 개인정보가 노출되도록 한 행위는 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	• 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)

나. 개인정보 유출 등의 통지·신고 조치를 하지 않은 행위

{보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)}

피심인은 개인정보의 유출 사실을 인지한 때로부터 24시간 이내에 유출 사실을 통지·신고하여야 하나, 정당한 사유 없이 24시간을 초과하여 유출통지·신고한 행위는 보호법 제39조의4제1항, 같은 법 시행령 제48조의4제2항을 위반한 것이다.

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

2) 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하거나 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 등 침입차단·탐지시스템을 운영하여야 한다.

3) 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

나. 피심인은 개인정보의 유출 사실을 인지한 때로부터 24시간 이내에 유출 사실을 통지·신고하여야 하고, 유출 사실에 대한 이용자 통지 시 법정 통지 항목을 모두 포함하여 통지하여야 한다.

다. 피심인은 가.와 나.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 과징금 부과

< ① 개인정보 유출 사건('22. 3. 16일, '22. 4. 8일 유출 신고건) >

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15 제1항제5호, 같은 법 시행령 제48조의11제1항과 제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 「개인정보보호 법규 위반에 대한 과징금 부과기준」(2020. 8. 5. 개인정보보호위원회 고시 제2020-6호, 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 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, 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단한다.'라고 규정하고 있다.

이에 따라, 보호법 제29조(안전조치의무)를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은 '정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 매우 중대한 위반행위로 판단한다.'라고 규정하고 있다.

다만, 과징금 부과기준 제5조제3항 단서에서 '위반행위의 결과가 ▲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 해당할 때에는 보통 위반행위로, 1개 이상 2개 이하에 해당하는 경우에는 중대한 위반행위로 감경한다.'라고 규정하고 있다.

이에 따라, ▲피심인이 위반행위로 인해 직접적인 이득을 취하지 않은 점, ▲이용자의 개인정보가 공중에 노출되지 않은 점을 고려하여 '중대한 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 관련 매출액은 온라인쇼핑몰 서비스를 통해 발생한 매출액으로 하고, 직전 3개 사업년도의 연평균 매출액 천 원에 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 천 원으로 한다.

※ 피심인은 B2B사업도 행하는 자로, B2B매출액(위반행위와 무관한 매출액)에 대한 객관적인 증빙자료를 제출할 것을 요청하였나 제출하지 않아 재무제표상 전체 매출액을 관련 매출액으로 산정함

< 피심인의 위반행위 관련 매출액 >

(단위: 천 원)

구 분	2019년	2020년	2021년	평 균
관련 매출액				

* 피심인이 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('16. 1. 29. ~ '22. 4월)하는 '장기 위반행위'에 해당하므로 기준금액의 100분의 50에 해당하는 금액인 천 원을 가산하고,

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

라. 추가적 가중 및 감경

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

이에 대해 특별히 가중할 사유는 없으며, 피심인이 ▲조사에 적극 협력한 점, ▲개인정보 유출 사실을 자진 신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 천 원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15 제1항제5호, 같은 법 시행령 제48조의11, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 512,591천 원을 최종과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금
천 원	필수적 가중 (50% : 천 원) 필수적 감경 (50% : 천 원)	추가적 가중 없음 추가적 감경 (20%, 천 원)	**천 원**
	⇒ 천 원	⇒ 천 원	

3. 과태료 부과

피심인의 보호법 제29조, 제39조의4 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항 제4호·제6호 및 제3항제3호 및 같은 법 시행령 제63조의〔별표2〕'과태료 부과기준' 및「개인정보 보호법 위반에 대한 과태료 부과기준」(2021. 1. 27. 개인정보보호위원회 의결, 이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

< ① 개인정보 유출 사건('22. 3. 16일, '22. 4. 8일 유출 신고건) >

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 제29조(안전조치의무) 및 제39조의4(개인정보 유출등의 통지·신고에 대한 특례) 위반에 대해서는 1회 위반에 해당하는 과태료인 600만 원을 각각 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		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 보호법 제29조(안전조치의무) 위반행위에 대해 과태료 부과지침 제8조(과태료 가중기준)에 따라 ▲제3호(가중사유의 위반행위별 각 목의 세부기준)에서 정한 행위가 2개이며, ▲위반 기간이 3개월 이상인 경우로 위반행위별 기준금액의 20%를 가중하고,

보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해 과태료 부과지침 제8조(과태료 가중기준)에 해당하지 않아 가중 없이 기준금액을 유지한다.

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 ▲일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점, ▲사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정중에 있는 것으로 인정되는 점, ▲「중소기업기본법」제2조에 따른 중기업(中企業)에 해당하는 점 등을 종합적으로 고려하여 과태료 부과지침 제7조에 따라 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조, 제39조의4항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 720만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만 원	120만 원	300만 원	**420만 원**
개인정보 유출통지	600만 원	-	300만 원	**300만 원**
계				**720만 원**

< ② 개인정보 유출 사건('22. 5. 17일 유출 신고건) >

가. 기준금액

보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 피심인의 보호법 제29조(안전

조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례) 위반에 대하여 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 과태료인 600만 원을 각각 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		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 보호법 제29조(안전조치의무) 위반행위에 대해 ▲위반기간이 3개월 이상(간편로그인 기능 도입: '20. 4. 30. ~)인 경우로 기준금액의 10%를 가중하고, 보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해 위반의 정도와 관련하여 ▲제3호(가중사유의 위반행위별 각 목의 세부기준)에서 정한 행위가 2개인 경우로 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 ▲사소한 부주의 또는 시스템의 오류로 인한 것으로 인정되며 피해 발생이 없는 점, ▲일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점, ▲사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정중에 있는 것으로 인정되는 점, ▲「중소기업기본법」제2조에 따른 중기업(中企業)에 해당하는 점을 종합적으로 고려하여 과태료 부과지침 제7조에 따라 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 720만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만 원	60만 원	300만 원	**360만 원**
개인정보 유출통지	600만 원	60만 원	300만 원	**360만 원**
계				**720만 원**

4. 결과 공표

「개인정보 보호법」 제66조제1항 및 「개인정보보호위원회 처분 결과 공표기준」 (2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

<table>
<tr><td colspan="6">개인정보보호법 위반 행정처분 결과 공표
개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.</td></tr>
<tr><td rowspan="2">순번</td><td rowspan="2">위반행위를 한 자</td><td colspan="2" rowspan="2">위반행위의 내용</td><td colspan="2">행정처분의 내용 및 결과</td></tr>
<tr><td>처분일자</td><td>처분내용</td></tr>
<tr><td rowspan="2">1</td><td rowspan="2">명칭</td><td>위반조항</td><td>위반내용</td><td rowspan="2">2022. 8. 10.</td><td>시정조치 명령
과태료 780만 원</td></tr>
<tr><td>법 제29조</td><td>안전조치의무 위반
(접근통제)</td><td>시정조치 명령
과태료 660만 원</td></tr>
<tr><td colspan="6">법 제39의4
개인정보 유출통지·신고 위반
(지연통지·신고, 유출항목 누락 통지)

2022년 8월 10일
개 인 정 보 보 호 위 원 회</td></tr>
</table>

Ⅴ. 결론

피심인의 보호법 제29조, 제39조의4 위반행위에 대하여 같은 법 제39조의15(과징금의 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항제6호·제12호의3, 제64조(시정조치 등)제1항, 제66조(결과의 공표)제1항에 따라 과징금, 과태료, 시정조치, 결과 공표 명령을 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.

2022년 8월 10일

위 원 장　　윤 종 인　(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　　지 성 우　(서 명)