개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2023-011-114호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 (사업자등록번호 :)

대표자
의결연월일 2023. 6. 28.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 전사적 차원에서 개인정보 내부관리계획을 재정립하고, 정기적인 개인정보보호 교육 계획을 수립·이행하여야 한다.

나. 피심인은 개인정보 유출이 발생한 개인정보처리시스템을 포함하여 피심인이 운영 중인 개인정보처리시스템 전반에 대해 「개인정보 보호법」 제29조(안전조치의무) 준수 여부를 자체적으로 점검하고, 재발방지대책을 수립하여야 한다. 특히, 피심인은 침해사고 방지를 위해 개인정보처리시스템에 대한 불법적인 접근이 의심되는 IP주소 및 도용이 의심되는 계정 등을 재분석하여 개인정보 유출 시도를 탐지·차단하여야 한다.

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

2. 피심인 에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 원

나. 과 태 료 : 14,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

등을 통해 클라우드 서비스, 온라인 쇼핑몰 서비스 등을 제공하는 피심인은 「(구)정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2020. 8. 5. 법률 제16955호로 개정·시행되기 이전의 것, 이하 '정보통신망법'이라 한다.)에 따른 정보통신서비스 제공자이며, 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16930호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이고, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보포털(privacy.go.kr)에 총 6차례 유출 신고*('20. 1. 8., '20. 4. 10., '20. 4. 22., '20. 4. 29., '20. 5. 13., '21. 5. 7.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('20. 5. 12. ~ '21. 12. 21.)하였으며, 다음과 같은 사실을 확인하였다.

* 이 중 2건('20. 1. 8., '20. 4. 22. 유출 신고)은 조사 과정에서 의무 위반 정도가 처분까지 이르기에는 어렵다고 판단하여 종결하였으며, 2건('20. 4. 29., '20. 5. 13. 유출 신고)은 계정 도용을 통한 1·2차 공격으로 판단하여 함께 조사

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스( )를 운영하면서 '20. 7. 8. 기준으로 국내외 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보			
휴면 회원 정보			
합 계			

피심인은 서비스( )를 운영하면서 이용자의 개인정보를 수집하여 보관하고 있다.

< 에 동기화 및 백업될 수 있는 개인정보 >

구분	항목
동기화	
백업	

피심인은 서비스( )를 운영하면서 ’21. 6. 7. 기준으로 이용자 명의 이용자의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보			
합 계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

(1) ’20. 4. 10. 개인정보 유출 신고 관련

일시		피심인의 유출 인지·대응 내용

(2) ’20. 4. 29., ’20. 5. 13. 개인정보 유출 신고 관련

일시		피심인의 유출 인지·대응 내용

(3) ’21. 5. 7. 개인정보 유출 신고 관련

일시		피심인의 유출 인지·대응 내용

2) 유출경위 및 규모

(1) ’20. 4. 10. 개인정보 유출 신고 관련

① 유출 경위

피심인은 데이터베이스(이하, ‘DB') 간 데이터 처리방식의 차이에 대한 이해를 소홀히 하고 DB를 교체하여, 기존 이용자의 개인정보가 신규 가입 이용자의 개인정보로 잘못 변경됨에 따라 이용자의 개인정보가 유출되었다.

피심인은 ’20. 3. 8. DB에서 DB로 변경하는 과정에서 두 DB 간 데이터 처리 방식의 차이*를 인지하지 못하였다.

* DB는 ‘NULL’과 공백문자(“ ”) 모두 NULL로 인식하여 저장하는 반면, DB는 공백문자(“ ”)를 별도의 문자로 인식함

’20. 3. 8.부터 4. 6.까지 만 14세 미만 이용자*의 개인정보가 DB에 저장되는 과정에서 CI(Connecting Information : 연계 정보)값이 저장되는 DB 필드에 “NULL”이 아닌 공백 문자(“”)가 저장되었으며, 그 결과 CI값이 저장되는 DB 필드에 공백 문자(“”)가 저장되어 있던 기존 만 14세 미만 이용자 계정 260개의 개인정보(이름·생년월일)가 ’20. 3. 8. 이후 가입한 만 14세 미만 가입자 155명의 개인정보로 변경되었고, 이 중 최소 26명의 이용자가 내 ‘개인정보’ 메뉴까지 접속하여

다른 이용자 26명의 개인정보(이름·생년월일)를 열람하였다.

* 만 14세 미만 이용자는 본인인증을 하지 않아 'CI' 값이 없음

② 유출항목 및 규모

최소 이용자 26명의 이름, 생년월일이 유출된 것으로 확인되었다.

(2) '20. 4. 29., '20. 5. 13. 개인정보 유출 신고 관련

① 유출 경위

신원미상의 자(해커)가 알 수 없는 방법으로 획득한 이용자의 아이디·비밀번호로 로그인한 후 개인정보를 조회·다운로드하였다.

피심인은 '20. 1. 14.부터 이용자가 접속 시 휴대전화를 이용한 2차 인증을 도입하였으나, 2차 인증 없이 접속 가능한 기존 경로를 삭제하지 않고 유지하였다.

신원미상의 자는 '20. 2. 15.부터 4. 29.까지 알 수 없는 방법으로 획득한 아이디(이메일 주소 또는 전화번호)와 비밀번호를 이용하여 2차 인증이 없는 기존 접속 경로로 에 접속을 시도하였으며, 접속에 성공한 계정 6개 중 5개 계정의 사진과 동영상 등을 조회·다운로드하였다.

피심인은 그러한 사실이 없음에도 다른 기기에서 로그인되었다는 메시지를 받았다는 이용자의 민원을 접수하고, '20. 4. 29. 2차 인증 없이 접속할 수 있는 기존 접속 경로를 차단하였다.

신원미상의 자는 '20. 4. 29.부터 '20. 5. 11.까지 알 수 없는 방법으로 획득한 아이디와 비밀번호를 이용하여 의 2차 인증수단 설정 페이지에 접속을 시도하였고, 접속에 성공한 234개 계정 이용자의 2차 인증수단에 자신이 보유한 휴대전화번호(24개)를 설정하고, 71개 계정의 에 접속하여 사진과 동영상 등을 조회·다운로드하였다.

피심인은 그러한 사실이 없음에도 2차 인증 수단이 등록되었다는 이용자의 민원을 접수하고, '20. 5. 12. 2차 인증이 설정된 계정의 2차 인증을 초기화하였다.

② 유출항목 및 규모

최소 76개 계정에서 사진, 동영상 등이 유출된 것으로 확인되었다.

(3) ’21. 5. 7. 개인정보 유출 신고 관련

① 유출 경위

피심인의 개발 과정상 과실로 로그인 여부(세션)를 확인하는 로직을 누락시켜 이용자가 본인이 아닌 다른 이용자의 개인정보를 열람하였다.

피심인은 ’21. 3. 23. 온라인 스토어 기능 수정 작업 중 개발상 과실로 ‘주문 배송지 리스트’ 페이지에 로그인 여부(세션)를 확인하는 로직을 누락하였으며, 이로 인해, 회원 식별번호(*)가 ‘0’으로 동일한 배송지 정보가 총 65건(중복 3건 포함)이 생성되었다.

* 는 고객의 온라인 스토어 아이디와 1:1 맵핑하여 에서 자체적으로 관리하는 내부 식별번호로 고객이 온라인 스토어에 로그인 후 30분 이상 미이용으로 인하여 세션이 종료될 경우 세션값 중 회원 식별번호( )는 ‘0’으로 초기화됨

그 결과 이용자가 ’21. 5. 4. 온라인 스토어에 로그인하여 배송지 정보를 변경하는 과정에서 타인의 이름, 주소, 휴대전화번호 등 19명의 개인정보를 조회*(총 20건 조회, 1건 중복)하여 ’21. 5. 5. 피심인에게 민원을 제기하였고, 피심인은 ‘21. 5. 6. 관련 오류를 수정 조치하였다.

* 이용자는 온라인 스토어에 로그인하여 주문·배송 상세화면 접속 후 세션이 종료된 상태로 배송지를 변경하였고, 이 과정에서 이용자의 세션 정보 내 회원 식별번호가 '0'으로 설정되면서 회원 식별번호가 '0'으로 설정된 다른 이용자의 배송지 정보를 조회

② 유출항목 및 규모

최소 이용자 19명의 이름, 주소, 휴대전화번호가 유출된 것으로 확인되었다.

3. 개인정보의 취급.운영 관련 사실관계

가. ’20. 4. 10. 개인정보 유출 신고 관련 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ’20. 3. 8. DB 변경(DB → DB)과정에서 DB별 데이터 처리방식 차이에 대한 이해를 소홀히 하여, 기존 만 14세 미만 이용자 260명의 개인

정보가 ’20. 3. 8. 이후 가입한 만 14세 미만 가입자의 개인정보로 잘못 변경되었으며, 이 중 최소 26명의 이용자가 다른 이용자의 개인정보(이름, 생년월일)를 열람한 사실이 있다.

나. ’20. 4. 29., ’20. 5. 13. 개인정보 유출 신고 관련 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 자체 침입차단 방침 등에 따라 불법 접근이 의심되는 IP 주소를 차단하고, 계정의 비밀번호를 초기화하는 등의 조치를 하였으나, 계정 도용 등으로 로그인에 성공한 것으로 의심되는 계정에 대한 개인정보 유출 여부 등에 대해서는 분석하지 않은 사실이 있다.

※ 피심인은 크리덴셜 스터핑 공격 인지 후 ’20. 4. 9.부터 ‘20. 4. 12.까지 개의 IP 주소와 개의 아이디를 차단하고, ’20. 4. 21.부터 ‘20. 4. 23.까지 개의 IP 주소와 개의 아이디를 차단함

다. ’21. 5. 7. 개인정보 유출 신고 관련 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ’21. 3. 23. 온라인스토어 시스템 기능 수정 작업 중 개발상 과실로 ‘주문 배송지 리스트’ 페이지에 로그인 여부(세션)를 확인하는 로직을 누락하였으며, 이로 인해, 회원 식별번호(‘0’)가 동일한 배송지 정보가 총 65건(중복 3건 포함) 생성되었으며, 이용자가 ’21. 5. 4. 온라인스토어에 로그인하여 주문 배송지 정보를 변경하는 과정에서 회원 식별번호가 ‘0’으로 설정되어 있는 다른 이용자의 배송지 정보(이름, 주소, 휴대전화번호)를 열람한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’22. 4. 7. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’22. 4. 25. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 “정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 ‘개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치 · 운영(제2호)’ 등의 기술적 · 관리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제15조제2항은 “법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)’ 등의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장 · 관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다.”라고 규정하고 있다.

같은 법 시행령 제15조제6항은 “방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호, 이하 ‘방송통신위원회 고시’) 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있고, 특히 방송통신위원회 고시 4조제9항은 “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 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 ‘그 밖에 개인정보에 대한 접근통제를 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 ‘개인정보보호위원회 고시’) 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있고, 개인정보보호위원회 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.

2. 위법성 판단

가. ’20. 4. 10. 개인정보 유출 신고 관련 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[정보통신망법 제28조(개인정보의 보호조치)제1항]

피심인이 기존 DB와 신규 DB 제품 간 데이터 처리 방식의 차이를 고려하지 않고 DB 교체과정에서 개인정보의 정합성을 확인하지 않는 등 권한이 없는 자에게 개인정보가 공개되지 않도록 개인정보에 대한 접근통제를 위하여 필요한 조치를 소홀히 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호 및 방송통신위원회 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보의 보호조치 위반	정보통신망법 §28①	§15②	・열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(방송통신위원회 고시§4⑨)

나. '20. 4. 29., '20. 5. 13. 개인정보 유출 신고 관련 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[정보통신망법 제28조(개인정보의 보호조치)제1항]

피심인이 신원미상의 자가 도용한 것으로 의심되는 아이디와 비밀번호로 로그인에 성공한 이후 이용자의 개인정보가 조회·다운로드되었는지 여부 등에 대해 분석하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호 및 방송통신위원회 고시 제4조제5항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보의 보호조치 위반	정보통신망법 §28①	§15②	・불법적인 접근 및 침해사고 방지를 위한 개인정보 처리시스템에 대한 침입 탐지·차단 시스템 운영을 소홀히 한 행위(방송통신위원회 고시 §4⑤)

다. '21. 5. 7. 개인정보 유출 신고 관련 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인이 시스템 기능 수정 작업 시 로그인 여부를 확인하는 로직을 누락하는

등 개인정보에 대한 접근통제를 위하여 필요한 조치를 소홀히 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호 및 개인정보보호위원회 고시 제4조 제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§48의2①	・열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(개인정보보호위원회 고시§4⑨)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 전사적 차원에서 개인정보 내부관리계획을 재정립하고, 정기적인 개인정보보호 교육 계획을 수립·이행하여야 한다.

나. 피심인은 개인정보 유출이 발생한 개인정보처리시스템을 포함하여 피심인이 운영 중인 개인정보처리시스템 전반에 대해 「개인정보 보호법」 제29조(안전조치의무) 준수 여부를 자체적으로 점검하고, 재발방지대책을 수립하여야 한다. 특히, 피심인은 침해사고 방지를 위해 개인정보처리시스템에 대한 불법적인 접근이 의심되는 IP 주소 및 도용이 의심되는 계정 등을 재분석하여 개인정보 유출 시도를 탐지·차단하여야 한다.

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

2. 과징금 부과

가. '20. 4. 10., '20. 4. 29., '20. 5. 13. 개인정보 유출 신고 관련

피심인의 ’20. 4. 10. 개인정보 유출 신고 관련 정보통신망법 제28조제1항 위반행위 및 ’20. 4. 29., ’20. 5. 13. 개인정보 유출 신고 관련 같은 법 제28조제1항 위반행위는 각각 ‘이용자의 개인정보를 유출한 경우로서 정보통신망법 제28조제1항제2호의 조치를 하지 아니한 경우’에 해당하여 원칙적으로 각각 같은 법 제64조의3제1항제6호에 따른 과징금 부과 대상이다.

특히 모든 서비스에 이용되는 통합계정 서비스인 과 사생활 침해 가능성이 큰 사진과 동영상 등이 보관된 에서 개인정보가 유출되는 사고가 발생하였으나, 다만 각각의 경우 정보주체의 추가 피해가 확인되지 않았고 상대적으로 유출된 정보주체의 규모(26명, 76명)가 크지 않은 점 등을 고려하여 방송통신위원회 과징금 부과기준 제9조*에 따라 과징금 부과를 시정조치를 명령으로 갈음한다.

* 「개인정보 보호 법규 위반에 대한 과징금 부과기준」(방송통신위원회 고시, 제2019-12호, 이하 ‘방송통신위원회 과징금 부과기준’) 제9조는 위반 정도가 경미하다고 판단되는 경우에는 과징금 부과를 시정조치의 명령으로 갈음할 수 있다고 규정하고 있음

나. ’21. 5. 7. 개인정보 유출 신고 관련

피심인의 ’21. 5. 7. 개인정보 유출 신고 관련 보호법 제29조 위반행위는 ‘이용자의 개인정보를 유출한 경우로서 보호법 제29조의 조치를 하지 아니한 경우’에 해당하여 같은 법 제39조의15제1항제5호에 따른 과징금 부과 대상이다.

특히 비교적 짧은 기간 동안 유출 사고가 연속적·반복적으로 발생(’’20. 1. 8., ’20. 4. 10., ’20. 4. 22., ’20. 4. 29., ’20. 5. 13. 유출 신고)한 이후 또다시 유출 사고가 발생(’21. 5. 7. 유출 신고)하여 피심인이 ’20년 유출 사고 발생 이후 ’21년 유출 사고가 재발하기까지의 기간 동안 보호법 상의 안전조치의무 이행과 개인정보 보호체계의 점검·정비 등 재발방지 대책의 마련과 이행을 충실히 했다고 볼 수 없으며, “과징금 부과를 시정조치 명령으로 갈음하여 처분을 받았음에도 같은 위반행위로 적발된 개인정보처리자에게는 해당 과징금 미부과 사유를 재적용하지 아니한다.”라고 규정한 ‘경미한 위반행위에 대한 과징금 미부과 기준(’21. 9. 9. 개인정보보호위원회 의결)’의 취지 등을 고려하여 피심인의 ’20. 4. 10. 유출 신고 관련 정보통신망법

제28조제1항 위반행위 및 ’20. 4. 29., ’20. 5. 13. 유출 신고 관련 같은 법 제28조제1항 위반행위에 대해서는 과징금을 면제하되 피심인의 ’21. 5. 7. 유출 신고 관련 보호법 제29조 위반행위에 대해서는 과징금을 면제하지 않고 부과한다.

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 ‘개인정보보호위원회 과징금 부과기준‘이라 한다)’에 따라 다음과 같이 부과한다.

1) 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.

2) 기준금액

(1) 고의 · 중과실 여부

개인정보보호위원회 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.

이에 따를 때, 보호법 제29조의 안전조치의무를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

(2) 중대성의 판단

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

다만, 개인정보보호위원회 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 위반행위'로, 1개 이상 2개 이하에 해당하는 경우 '중대한 위반행위'로 감경하도록 규정하고 있다.

피심인의 경우, '위반행위로 인해 직접적으로 이득을 취하지 않은 경우', '위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우' 및 '이용자의 개인정보가 공중에 노출되지 않은 경우'에 해당하여 '보통 위반행위'로 감경한다.

(3) 기준금액 산출

피심인의 온라인 쇼핑몰( )을 통해 발생한 매출을 위반행위 관련 매출로 하고, 직전 3개 사업년도의 연평균 매출액 천원에 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율 1천분의 15를 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2018년	2019년	2020년	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**

3) 필수적 가중 및 감경

개인정보보호위원회 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 1년 이내 ('21. 3. 24. ~ '21. 5. 6.)이므로 '단기 위반행위'에 해당하여 기준금액을 유지하고, 최근 3년 이내 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 적이 없으므로 기준금액의 100분의 50에 해당하는 천원을 감경한다.

4) 추가적 가중 및 감경

개인정보보호위원회 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 ▲조사에 협력한 점, ▲개인정보 유출사실을 자진 신고한 점 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 천원을 감경한다.

5) 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 개인정보보호위원회 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 천원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중 · 감경	추가적 가중 · 감경	최종 과징금
천원 (보통 위반)	① 기준금액 유지 (단기 위반) ② 기준금액 50% 감경 (최초 위반 : 천원)	필수적 가중·감경 거친 금액의 20% 감경(천원)	천원

3. 과태료 부과

가. ’20. 4. 10., ’20. 4. 29., ’20. 5. 13. 개인정보 유출 신고 관련

피심인의 ’20. 4. 10. 유출 신고 관련 정보통신망법 제28조(개인정보의 보호조치) 제1항 위반행위 및 ’20. 4. 29., ’20. 5. 13. 유출 신고 관련 같은 법 제28조제1항 위반행위에 대한 과태료는 같은 법 제76조제1항제3호와 같은 법 시행령 제74조, 같은 법 시행령 [별표9] ‘과태료의 부과기준’, ‘개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침(이하 ‘방송통신위원회 과태료 부과지침’)’에 따라 다음과 같이 부과한다.

1) 기준금액

정보통신망법 시행령 제74조의 [별표9]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 ’20. 4. 10. 유출 신고 관련 같은 법 제28조제1항 위반행위 및 ’20. 4. 29., ’20. 5. 13. 유출 신고 관련 같은 법 제28조제1항 위반행위에 대해 기준금액을 1회 위반에 해당하는 1,000만원으로 각각 산정한다.

< 정보통신망법 시행령 [별표9] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	정보통신망법 제76조 제1항제3호	1,000	2,000	3,000

2) 과태료의 가중 및 감경

(1) 과태료의 가중

방송통신위원회 과태료 부과지침 제8조는 ‘사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲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, ’20. 4. 10. 유출 신고 관련 정보통신망법 제28조제1항 위반행위 및 ’20. 4. 29., ’20. 5. 13. 유출 신고 관련 같은 법 제28조제1항 위반행위는 방송통신위원회 과태료 부과지침 제8조 및 [별표2] 과태료의 가중기준에서 정한 가중사유가 없으므로 기준금액을 유지한다.

(2) 과태료의 감경

방송통신위원회 과태료 부과지침 제7조는 ‘사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲사업규모·자금사정, ▲개인정보보호 노력정도, ▲조사협조 및 자진시정, ▲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, ’20. 4. 10. 유출 신고 관련 정보통신망법 제28조제1항 위반행위는 방송통신위원회 과태료 부과지침 제7조 및 [별표1] 과태료의 감경기준에 따라 ‘위반행위에 대해 시정을 완료한 경우’ 및 ‘조사에 협력한 경우’에 해당하여 기준금액의 50%인 500만원을 감경하고, ’20. 4. 29., ’20. 5. 13. 유출 신고 관련 같은 법 제28조제1항 위반행위는 방송통신위원회 과태료 부과지침 제7조 및 [별표1] 과태료의 감경기준에 따라 ‘조사에 협력한 경우’에 해당하여 기준금액의 40%인 400만원을 감경한다.

3) 최종 과태료

피심인의 ’20. 4. 10. 유출 신고 관련 정보통신망법 제28조제1항 위반행위 및 ’20. 4. 29., ’20. 5. 13. 유출 신고 관련 같은 법 제28조제1항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,100만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
'20. 4. 10. 유출 신고 관련 개인정보의 보호조치 의무 위반	1,000만원	-	500만원	**500만원**
'20. 4. 29., '20. 5. 13. 유출 신고 관련 개인정보의 보호조치 의무 위반	1,000만원	-	400만원	**600만원**
계				**1,100만원**

나. '21. 5. 7. 개인정보 유출 신고 관련

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과태료는 같은 법 제75조 제2항제6호, 같은 법 시행령 제63조, 같은 법 시행령 [별표2] '과태료의 부과기준' 및 '개인정보 보호법 위반에 대한 과태료 부과기준'(이하 '개인정보보호위원회 과태료 부과지침')에 따라 다음과 같이 부과한다.

1) 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 보호법 제29조 위반행위에 대해 기준금액을 1회 위반에 해당하는 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	보호법 제75조 제2항제6호	600	1,200	2,400

2) 과태료의 가중 및 감경

(1) 과태료의 가중

개인정보보호위원회 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 위반행위는 개인정보보호위원회 과태료 부과지침 제8조 및 [별표2] 과태료의 가중기준에서 정한 가중사유가 없으므로 기준금액을 유지한다.

(2) 과태료의 감경

개인정보보호위원회 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, 보호법 제29조 위반행위는 개인정보보호위원회 과태료 부과지침 제7조 및 [별표1] 과태료의 감경기준에 따라 '위반행위에 대해 시정을 완료한 경우' 및 '조사에 협력한 경우'에 해당하여 기준금액의 50%인 300만원을 감경한다.

3) 최종 과태료

피심인의 보호법 제29조 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 300만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반	600만원	-	300만원	**300만원**

Ⅴ. 결론

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 및 보호법 제29조(안전조치의무)를 위반한 행위에 대하여 보호법 제39조의15(과징금의 부과 등에 대한 특례)제1항제5호, 정보통신망법 제76조(과태료)제1항제3호, 보호법 제75조(과태료)제2항제6호, 같은 법 제64조(시정조치 등)제1항에 따라 과징금·과태료 부과, 시정조치 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 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.

2023년 6월 28일

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)