

제 12 회 개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의 · 의결

안 건 번 호 제2023-212-220호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2023. 6. 14.

주 문

1. 피심인 에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

I. 기초 사실

온라인 의류 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 개인정보 포털(privacy.go.kr)에 유출 신고('22. 4. 26.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('22. 11. 18. ~ '23. 2. 9.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 온라인 의류 쇼핑몰()을 운영하면서 '22. 12. 5. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보	(필수) 성명, 생년월일, 핸드폰번호, 성별, 비밀번호, 이메일 (선택) 전화번호, 배송지, 환불계좌, 추천인 아이디 및 이름, 신체 사이즈	'22. 4. 1. ~ 계속	(유효) (분리)
합 계			

※

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
'22. 4. 22.	-	쇼핑몰 내 통합회원번호 변경작업 진행
'22. 4. 25.	09:17	타인의 주문정보가 보인다는 이용자 민원 접수 및 내부 분석 개시
'22. 4. 26.	10:26	2명의 주문정보가 유출된 사실을 확인하며 개인정보 유출 인지 및 정상 업데이트 처리
	11:53	개인정보보호 포털을 통한 개인정보 유출신고
	14:27	이용자 대상 개인정보 유출통지

2) 유출항목 및 규모

이용자 2명의 이름·휴대전화번호·이메일·주소가 유출되었다.

※ 잘못 업데이트된 회원정보는 총 111건이나, 오류 발생기간의 로그인 기록 등을 분석한 결과, 로그인한 2명에게 다른 2명의 개인정보만 각각 유출되었음을 확인하였음

3) 유출경위

쇼핑몰의 기존 회원정보를 신규 쇼핑몰로 이전하면서, 신규 회원의 '주문테이블 회원정보' 항목에 신규 통합회원번호가 아닌 기존 이용자의 회원번호를 업데이트하여,

신규 회원이 통합 쇼핑몰 로그인 시, 기존 이용자의 주문정보*가 노출되는 오류가 발생하였다.

* 주문정보는 단순 구매이력 정보로 결제정보 등은 미포함

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 온라인 의류 쇼핑몰을 운영하면서, DB 주문정보 테이블에 회원정보 데이터를 오입력하여, 로그인 시 타인의 주문정보가 표출되어 이용자의 개인정보가 유출된 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '23. 2. 13. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '23. 2. 24. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법 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 “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 제2021-3호, 이하 ‘고시’) 제4조제9항은 “정보통신서비스 제공자들은 처리 중인 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. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인이 온라인 의류 쇼핑몰을 운영하면서, DB 주문정보 테이블에 회원정보 데이터를 오입력하여, 로그인 시 타인의 주문정보가 표출되어 이용자의 개인정보가 유출되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§48의2① 제2호	• 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(고시§4⑨)

IV. 처분 및 결정

1. 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’(2021. 1. 27. 개인정보보호위원회 의결, 이하 ‘과태료 부과지침’)에 따라 다음과 같이 과태료를 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 위반행위 기준금액을 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, 제28조의4 제1항 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 과태료 부과기준 제8조(과태료 가중기준)에 해당하지 않아 가중없이 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, ▲위반 정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위

반행위의 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 행위는 과태료 부과지침 제7조 및 [별표1] 과태료의 감경기준에 따라, ‘위반행위에 대해 시정을 완료한 경우’에 해당하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 300만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만원	-	300만원	300만원
계				300만원

V. 결론

피심인의 보호법 제29조(안전조치의무)를 위반한 행위에 대하여 같은 법 제75조(과태료)제2항제6호에 따라 과태료 부과를 주문과 같이 의결한다.

이의제기 방법 및 기간

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 14일

위 원 장 지 성 우 (서명)

위 원 강 정 화 (서명)

위 원 염 홍 열 (서명)