

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

안 건 번 호 제2023-212-219호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2023. 6. 14.

주 문

1. 피심인 에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인 에 대한 과태료 부과 내용 및 결과를 개인정보보호
위원회 홈페이지에 공표한다.

이 유

I. 기초 사실

화장품 쇼핑몰 서비스 등을 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. 3. 22.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('22. 12. 29. ~ '23. 5. 2.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 화장품 쇼핑몰()을 운영하면서 ' 23. 2. 15. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집 현황 >

구분	항목	수집일	건수
합 계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지 및 대응 내용
'22. 3. 19.	19:14	이용자 A가 으로 구글 검색엔진에서 홈페이지 내 특정 페이지가 노출된다는 문의메일(관련 첨부 파일 2개 포함) 발송(1차)
'22. 3. 21.	11:32	이용자 A가 으로 구글 검색엔진에서 홈페이지 내 특정 페이지가 노출된다는 문의 메일 발송(1차와 동일 내용·중복)(2차)
	12:12	이용자 A가 으로 개인정보 유출 관련 문의 메일* 발송 * 이용자 A는 구글 검색 시, 홈페이지의 특정 페이지에서 타 이용자의 개인정보가 조회된 이미지를 첨부함
	12:34	피심인이 이용자 A의 메일 내용 확인 후, 사고 경위 파악 진행(인지시점)
'22. 3. 22.	11:55~12:04	개인정보가 유출된 고객에게 유출 사실 통지(전화)
	12:31	개인정보 포털에 개인정보 유출 신고
	13:12	마스킹된 이름이 유출된 이용자에게 유출 사실 통지(문자, 14명)
	18:22~	유출 관련 오류 사항에 대한 개선 조치

2) 유출항목 및 규모

이용자 1명의 이름.주소, 1명의 이름.주소.휴대전화번호(총 2명)가 유출되었다.

3) 유출 경위

피심인은 '제품문의 게시글'에 대한 소스코드 설정 오류, 해당 웹페이지에 대한 검색엔진(구글) 크롤링 설정 및 비정상 호출 차단 조치를 소홀히 하여 개인정보가 유출되었다.

피심인은 쇼핑몰 홈페이지 내 제품문의 페이지의 게시글을 타인이 볼 수 없도록 비공개로 설정·운영하였으나, 해당 비공개 설정을 관리자 외의 자가 해제(수정)할 수 없도록 조치*하지 않았다.

* 게시글을 작성자 본인 외의 자가 볼 수 없도록 비공개 설정(lock)하였으나, 누구든지 해당 웹페이지의 '개발자 도구' 설정 항목에서 잠금(lock) 처리된 설정(소스코드)을 해제(수정)할 수 있었음

아울러 피심인은 구글 검색로봇에 의해 제품문의 페이지가 크롤링 되지 않도록 조치하지 않았으며, 해당 페이지에 대한 정상적인 접근*이 아닐 경우, 제품문의 글이 호출되지 않도록 조치하지 않아 '제품문의 게시판'이 구글에 크롤링 되었다.

* 해당 페이지를 호출하기 위한 필수 파라미터 값(상품 코드, 페이지 번호, 전체 리스트 개수) 없이 URL(https://www.)을 직접 입력하여 접속할 경우, 정상적인 접근이 아니므로 제품문의 페이지가 호출되지 않아야 함

이에 따라, 제품문의 게시글에 개인정보를 포함해 작성한 2명의 개인정보가 유출되었다.

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 홈페이지 내 비공개로 설정된 '제품문의 페이지'의 게시글이 권한 없는 자에게 공개되지 않도록 기술적 조치하지 않고, 해당 페이지에 대한 검색엔진(구글) 크롤링 및 비정상적인 호출 차단 조치를 소홀히 하여 이용자의 개인정보가 유출된 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '23. 5. 2. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '23. 5. 17. 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 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘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 제공자 등은 처리 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보 취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피식인이 제품문의 페이지의 게시글을 열람 권한이 없는 자가 볼 수 없도록 조치하지 않고, 해당 페이지에 대한 검색엔진 크롤링 및 비정상적인 호출 차단 조치를 소홀히 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

< 피식인의 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

피식인의 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’(이하 ‘과태료 부과지침’)에 따라 다음과 같이 부과한다.

가. 기준금액

보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반횟수에 따라 기준금액을 규정하고 있고, 피식인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위의 기준금액을 600만 원으로 산정한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수 별 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

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, ‘법 위반상태의 기간이 3개월 이상인 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, ▲사업 규모, ▲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, ‘과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반

행위를 중지하는 등 시정을 완료한 경우', '조사에 적극 협력한 경우'에 해당하여
기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐
총 360만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만원	60만원	300만원	360만원

2. 결과 공표

보호법 제66조제1항 및 ‘개인정보보호위원회 처분결과 공표기준’(2020. 11. 18.
개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 ‘위반
행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)’에 해당하므로
피심인이 과태료 부과를 받은 사실에 대해 개인정보보호위원회 홈페이지에 공표
한다.

개인정보보호법 위반 행정처분 결과 공표					
개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		법 제29조	안전조치의무 위반	2023.6.14.	과태료 부과 360만원
2023년 6월 14일 개 인 정 보 보 호 위 원 회					

V. 결론

피심인의 보호법 제29조(안전조치의무)를 위반한 행위에 대하여 같은 법 제75조(과태료)제2항제6호, 제66조(결과의 공표)제1항에 따라 과태료 부과, 결과 공표를 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)