

개 인 정 보 보 호 위 원 회

심의 · 의결

안 건 번 호 제2022-018-154호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2022. 11. 16.

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. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

I. 기초 사실

피심인은 사업자 전용(B2B) 휴대폰 액세서리 쇼핑몰을 운영하는 「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 피심인이 쇼핑몰 사이트를 통해 수집한 회원정보를 회원 동의 없이 별도 웹사이트 구축에 이용하고 안전조치를 소홀히 했다는 민원신고 ()를 접수함에 따라 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2022. 4. 25. ~ 2022. 8. 29.)하였으며, 다음과 같은 사실을 확인 하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 사업자 전용(B2B) 휴대폰 액세서리 쇼핑몰 웹사이트를 운영하면서 '22. 5. 12. 기준 전의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보	(필수) 아이디, 비밀번호, 이름, 휴대폰 번호 또는 전화번호, 이메일, 배송주소, 사업자정보(업체명, 사업자등록번호, 대표자명, 업태 등)		

나. 사이트 운영현황

1) 피심인은 '쇼핑몰'과 '맵' 사이트를 운영 중임

- 쇼핑몰 : 이용자가 회원가입(개인회원*, 기업회원) 후 제품을 구매할 수 있는 사이트

* 기업회원으로 가입하지 못한 휴대폰 대리점·판매점의 소속 직원을 말하며, 휴대폰 대리점 등의 직원임이 확인된 경우에만 쇼핑몰 이용 가능

- 맵 : '쇼핑몰'을 통해 수집한 기업회원 정보를 지도에 표시한 사이트*로서, 피심인의 영업사원이 영업활동**에 이용함

* 개인회원은 맵에 표시되지 않으며, 기업회원 정보에는 휴대폰 대리점·판매점 담당 직원의 이름, 휴대폰번호 등 개인정보가 포함되어 있음[일반 이용자(쇼핑몰 회원)는 맵에 접근(접속·이용 등)할 수 없음]

** 피심인의 영업사원은 휴대폰 대리점 등의 위치를 확인하고 방문하여 휴대폰 액세서리 제품 소개 전단지(카탈로그) 및 제품 샘플 배부 등의 활동을 함

2) 피심인은 '쇼핑몰'에서 개인정보 수집 시 고지한 목적*과 동일하게 개인정보를 이용하여 '맵'을 운영하고 있으므로, 맵 운영을 위해 이용자로부터 별도 동의를 받지 않음

* 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 콘텐츠 제공

※ 맵은 쇼핑몰을 통해 수집한 개인정보를 지도 형태로 표시한 것에 불과함

3) 피심인은 휴대폰 대리점·판매점을 대상으로 영업업무를 수행하는 직원*에 대해 맵 접근권한을 부여함

* 피심인 소속 정규직원(업무총괄자) 1명, 영업 수행을 위해 피심인과 업무 위탁계약을 체결한 개인사업자 6명에게 접속·이용 권한 부여

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 영업사원이 외부에서 맵에 접속 시, 2차 인증 등 없이 아이디·비밀번호만으로 접속되도록 운영한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022. 8. 30. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2022. 9. 15. 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 ‘침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ‘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 세부기준은 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’라 한다) 제4조제4항은 “정보통신서비스 제공자등은 개인정보 취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위[보호법 제29조 (안전조치의무) 중 접근통제]

피심인이 외부에서 개인정보처리시스템에 접속 시 2차 인증 등 안전한 인증수단을 적용하지 않고 아이디·비밀번호만으로 접속하도록 운영한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제4항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	보호법 §29	§48조의2① 제2호	• 외부에서 개인정보처리시스템에 접속 시, 안전한 인증수단을 적용하지 않은 행위(고시§4④)

IV. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항 제6호, 같은 법 시행령 제63조의 [별표2] ‘과태료 부과기준’ 및 「개인정보 보호법 위반에 대한 과태료 부과기준(2021. 1. 27. 개인정보보호위원회 의결, 이하 ‘과태료 부과기준’이라 한다)」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 1회 위반에 해당하는 과태료인 600만 원을 적용한다.

< 「보호법」 시행령 [별표2] 2. 개별기준 >

(단위:만원)

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 부과기준 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 경우에 해당하여 기준금액의 10%를 가중한다.

2) **(과태료의 감경)** 과태료 부과기준 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 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위에 대한 시정을 완료한 점, 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 점, 사업규모가 「중소기업기본법」에 따른 소기업(小企業)인 점을 고려하여 기준금액의 50%를 감경한다.

다. 최종 과태료

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

< 과태료 산출내역 >

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

3. 결과 공표

보호법 제66조제1항 및 「개인정보보호위원회 처분결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 위반행위 시점을 기준으로 위반 상태가 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인에 대한 과태료 부과 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표				
개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.				
위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
명칭	위반조항	위반내용	처분일자	처분내용
	법 제29조	안전조치의무	2022.11.16.	과태료 부과 360만원

V. 결론

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조(과태료)제2항 제6호, 제66조(결과의 공표)제1항에 따라 과태료, 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.

2022년 11월 16일

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)