개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2023-004-035호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2023. 3. 8.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

   가. 피심인은 개인정보의 유출 사실을 안 때에는 지체없이 유출된 개인정보 항목, 유출이 발생한 시점, 이용자가 취할 수 있는 조치, 정보통신서비스 제공자 등의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 등을 해당 이용자에게 알려야 한다.

   나. 피심인은 가.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 : 9,600,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

3. 피심인 에 대한 시정조치 명령과 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

온라인 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 개인정보종합포털(privacy.go.kr)에 유출 신고('21. 6. 4.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('22. 10. 26. ~ '22. 11. 14.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 온라인 쇼핑몰(　　)를 운영하면서 '21. 9. 9. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보		~ 계속	
합 계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출 인지·대응 내용
‘21. 5. 11.	10:30	관리자 페이지 비밀번호 불일치 및 회사계정을 통한 스팸문자 발송 등 이상징후에 대해 호스팅사 문의
‘21. 5. 12.	14:50	호스팅사 답변 및 유출 가능성을 고려하여 KISA에 기술지원 요청
‘21. 5. 29.	00:10~ 03:35	해커가 회원 주문정보가 포함된 DB 다운로드
‘21. 6. 3.	18:02	KISA 기술지원 보고서 확인 후, 개인정보 유출인지
‘21. 6. 4.	14:12	개인정보보호 포털을 통한 개인정보 유출신고
	17:33	홈페이지 공지사항을 통한 개인정보 유출통지

2) 유출규모 및 경위

(유출항목 및 규모) 이용자 명*의 이름·전화번호·휴대전화번호·주소·이메일 등

* 회원정보가 아닌 주문정보 테이블이 유출되어 중복값을 제거한 수치로, 전자상거래법 상 보존정보(5년) 및 비회원 주문 건 등이 포함되어, 탈퇴 등을 반영한 현재 보유 회원정보 수와 차이 발생

(유출 경위) 해커가 웹셸* 공격을 통해 확보한 것으로 추정**되는 계정정보를 통해 개인정보처리시스템에 접속 및 주문정보를 다운로드하여 이용자의 개인정보가 유출됨

* 웹셸(Webshell) : 업로드 취약점을 통하여 시스템에 명령을 내릴 수 있는 악성 코드

** 계정정보 탈취 관련 다수의 웹셸 실행로그는 기록되어 있으나, 접속기록 보유기간 경과로 해당 웹셸의 업로드 경위·수행 작업 등은 확인 불가

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 온라인 쇼핑몰을 운영하면서, 개인정보 처리시스템에 대한 접속 권한을 IP주소 등으로 제한하지 않고, 웹셸이 업로드되어 실행되도록 하는 등 접근통제를 소홀히 하여 이용자 개인정보가 유출되도록 한 사실이 있다.

나. 개인정보 유출 통지를 소홀히 한 행위

피심인은 ’21. 6. 3. 한국인터넷진흥원 기술지원 보고서를 통해 개인정보 유출 인지 후, 유출된 이용자가 특정되지 않아 홈페이지 공지사항을 통해 유출통지한 바 있으나, 조사과정에서 유출이 확인된 이용자 명을 대상으로 개별 유출 통지하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’22. 10. 26. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’22. 11. 14. 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 “개인정보처리시스템에 대한 침입차단 시스템 및 침입탐지시스템의 설치·운영(나목)”, “그 밖에 개인정보에 대한 접근 통제를 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 ‘고시’) 제4조제5항은 “정보통신서비스 제공자등은 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 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

나. 보호법 제39조의4제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 유출등이 된 개인정보 항목(제1호), 유출등이 발생한 시점(제2호), 이용자가 취할 수 있는 조치(제3호), 정보통신서비스 제공자등의 대응 조치(제4호), 이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)를 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.”라고 규정하고 있다.

같은 법 시행령 제48조의4제2항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.”라고 규정하고 있으며, 제3항은 “정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.”라고 규정하고 있다

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인은 온라인 쇼핑몰을 운영하면서 개인정보 처리시스템에 대한 접근제한, 웹셸 업로드 및 실행 제한 등의 접근통제를 소홀히 하여 개인정보가 유출되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항 및 제9항을 위반한 것이다.

나. 개인정보 유출 통지를 소홀히 한 행위

[보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항]

피심인이 당초 유출된 이용자 정보가 특정되지 않아 홈페이지 공지사항을 통해 유출통지 하였으나, 조사과정에서 확인된 이용자 명을 대상으로 별도의 유출통지를 하지 않은 행위는 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§48의2① 제2호	• 개인정보 처리시스템에 대한 접속권한 제한 등 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 조치를 취하지 않은 행위(고시§4⑤) • 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(고시§4⑨)
개인정보 유출등의 통지·신고에 대한 특례 위반	보호법 §39의4①	§48조의4	• 정당한 사유 없이 개별 이용자 대상 유출통지를 하지 않은 행위

Ⅳ. 처분 및 결정

1. 과징금 부과

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

가. 과징금 상한액

피심인의 보호법 제29항 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, 같은 법 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

보호법 제29조의 안전조치의무를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있다.

다만, 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 3개에 해당하는 경우 '보통 위반행위'로, 1~2개에 해당하는 경우 '중대한 위반행위'로 감경하도록 규정하고 있다.

피심인의 경우 위반행위로 인해 직접적으로 이득을 취하지 않은 경우, 이용자의 개인정보가 공중에 노출되지 않은 경우에 해당하여 '중대한 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 '중대한 위반행위'의 부과기준율 1천분의 21을 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

다. 필수적 가중 및 감경

과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 1년 이내로 '단기 위반행위'에 해당하므로 기준금액을 유지하고,

최근 3년 이내 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 천원을 감경한다.

라. 추가적 가중 및 감경

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.

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

마. 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 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 천원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중 · 감경	추가적 가중 · 감경	최종 과징금
천원	필수적 가중(금액유지) 필수적 감경 (50% : 천원)	추가적 가중없음 추가적 감경 (20%, 천원)	**천원**
	→ 천원	→ 천원	

2. 과태료 부과

피심인의 보호법 제29조(안전조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제12호의3, 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 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 각 위반행위별 기준 금액을 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	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, 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위는 과태료

부과지침 제8조에 해당하지 않아 가중 없이 기준금액을 유지하고, 개인정보 유출 통지를 소홀히 한 행위는 '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, ▲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, 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위는 '위반행위에 대해 시정을 완료한 경우'에 해당하여 기준금액의 50%를 감경하고, 유출 통지를 소홀히 한 행위는 과태료 부과지침 제7조에 해당하지 않아 기준금액을 유지한다.

다. 최종 과태료

피심인의 보호법 제29조 및 제39조의4제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 960만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만원	-	300만원	**300만원**
개인정보 유출등의 통지·신고에 대한 특례	600만원	60만원	-	**660만원**
계				**960만원**

3. 결과 공표

보호법 제66조제1항 및 ‘개인정보보호위원회 처분결과 공표기준’(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 ‘법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우’(제4호)에 해당하므로 피심인에 대한 시정조치 명령과 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표				
위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	위반조항	위반내용	처분일자	처분내용
	법 제29조	안전조치의무 위반	2023.3.8.	과태료 부과 300만원
	법 제39조의4제1항	유출 통지·신고에 대한 특례 위반	2023.3.8.	과태료 부과 660만원 시정명령

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 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 부과, 시정조치 명령 및 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.

2023년 3월 8일

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)