개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2022-012-087호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2022. 7. 13.

주 문

1. 피심인 에 대하여 다음과 같이 과징금 및 과태료를 부과한다.

   가. 과 징 금 : 원
   나. 과 태 료 : 7,800,000원
   다. 납부기한 : 고지서에 명시된 납부기한 이내
   라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

쇼핑몰(,) 및 쇼핑앱( )을 운영하는 피심인은 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16955호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보보호포털(privacy.go.kr)에 유출 신고('21. 10. 22.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('21. 11. 23. ~ '22. 5. 26.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

쇼핑몰(,) 및 쇼핑앱( )을 운영하는 피심인은 '21. 12. 6. 기준으로 6,045,382건의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	- (필수) ID, 이메일, 휴대전화번호 - (선택) 생년월일, 성별, 프로필 이미지, 닉네임	'15. 2. 11. ~ '21. 12. 6.	(유효) 4,619,663 (분리보관) 1,425,719

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
'21. 10. 22.	08:00	한국인터넷진흥원으로부터 개인정보 판매 관련 다크웹 게시글 확인요청 메일 수신
	10:00	서비스 보안점검 및 유출 추정경로 차단
	17:00	개인정보보호 포털을 통한 개인정보 유출신고
'21. 10. 25.	17:00	전체 이용자 대상 개인정보 유출통지
'21. 11. 25.	-	AWS로부터 접속기록을 제공받아 세부 개인정보 유출경위 확인

2) 유출규모 및 경위

(유출항목 및 규모) ID·비밀번호(암호화)·이메일 등 개인정보 6,395,270건*

* 신원 미상의 자가 다크웹에 공개한 개인정보 파일을 기준으로 산정

(유출 경위) 신원 미상의 자가 알 수 없는 방법으로 확보한 AWS Access key를 이용하여, '21. 8. 29. ~ 30. 기간 동안 데이터베이스 임시저장 파일이 보관되어 있던 AWS S3(저장장치)에 접근*하여 개인정보를 조회·유출함

* '21. 8. 29. 15:51부터 '21. 8. 30. 17:41 기간동안 스웨덴IP(80.78.23.194), 독일IP(94.130.19.36)에서 AWS CLI(시스템 운영·관리 프로그램)를 통해 피심인의 AWS S3에 무단 접근한 후 DB 조회·유출

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 서비스 운영 목적으로 AWS S3(저장장치)에 접근할 수 있는 Access Key를 발급하는 과정에서 개인정보처리시스템에 대한 접속 권한을 아이피(IP) 등으로 제한하지 않았으며

데이터베이스 임시 저장파일이 저장되는 AWS S3에 대한 접속기록을 별도 저장하지 않은 사실이 있다.

※ 다만 는 AWS로부터 신원 미상의 자가 접속한 데이터베이스 테이블 등이 포함된 접속기록을 제공받아('21.11.25.) 제출하였으며, 이를 통해 세부적인 개인정보 유출 경위 파악

나. 탈퇴한 이용자의 개인정보를 파기하지 않은 행위

피심인은 개인정보처리방침을 통해 회원 탈퇴 시 30일 동안 분리보관되며 이후 파기한다고 안내하면서도, 현장조사일('21.12.7.) 기준 탈퇴한 회원 324,169명의 아이디(ID), 이메일 등을 파기하지 않고 보관한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '22. 5. 31. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '22. 6. 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.

보호법 시행령 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’ 등의 조치를 하여야 한다.”라고 규정하고 있으며

제48조의2제1항제3호는 “접속기록의 위조·변조 방지를 위하여 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등을 저장 및 이의 확인·감독(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

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 제5조제1항은 “정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존.관리하여야 한다.”라고 규정하고 있다.

나. 보호법 제21조제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.”고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

1) (접근통제) 피심인이 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항을 위반한 것이다.

2) (접속기록의 위·변조방지) 피심인은 개인정보취급자가 개인정보처리시스템(웹서버 및 DB 서버)에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않았고, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하지 아니한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제3호, 고시 제5조제1항을 위반한 것이다.

나. 탈퇴한 이용자의 개인정보를 파기하지 않은 행위

[보호법 제21조(개인정보의 파기)제1항]

피심인이 회원 탈퇴 등으로 불필요해진 개인정보에 대해 지체없이 파기하여야 하나 탈퇴한 계정 324,169건의 개인정보를 즉시 파기하지 않고 보관한 행위는 보호법 제21조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제, 접속기록)	보호법 §29	§48의2① 제2호·제3호	• 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하지 않은 행위 (고시§4⑤) • 개인정보취급자의 개인정보처리시스템 접속기록을 보관 및 점검을 소홀히 한 행위(고시§5①)
개인정보 파기 위반	보호법 §21①	§16	• 처리목적 달성 등 개인정보가 불필요하게 되었음에도 지체없이 파기하지 않은 행위

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 위반행위에 대해 보호법 제39조의15제1항5호의 이용자의 개인정보가 유출된 경우로서 개인정보의 안전조치의무(제29조)를 하지 않은 경우에 해당하여, 같은 법 시행령 제48조의11제1항·제3항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 '개인정보보호 법규 위반에 대한 과징금 부과기준'(개인정보보호위원회 고시 제2020-6호, 이하 '과징금 부과기준')에 따라 다음과 같이 과징금을 부과한다.

가. 과징금 상한액

피심인의 위반행위에 대한 과징금 상한액은 보호법 제39조의15제1항, 같은 법 시행령 제48조의11제1항에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액의 100분의 3이하에 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, 시행령

제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단한다.”라고 규정하고 있다.

피심인은 영리를 목적으로 정보통신망을 통해 정보통신서비스를 제공하는 자이며 보호법 시행령 제48조의2에 따른 안전성 확보조치를 이행하지 않은 사실이 있으므로 피심인에게 고의 또는 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은 “위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 매우 중대한 위반행위로 판단한다.”라고 규정하고 있다.

다만, 과징금 부과기준 제5조제3항 단서에서 위반행위의 결과가 ▲위반 정보통신서비스 제공자 등이 위반행위로 인해 직접적으로 이득을 취하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자 등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호)’ 중 모두에 해당하는 경우에는 보통 위반행위로, 1개 이상 2개 이하에 해당하는 경우에는 중대한 위반행위로 감경한다.”라고 규정하고 있다.

이에 따라 피심인이 개인정보 유출로 직접적인 이득을 취하지 않은 점을 고려하여 ‘중대한 위반행위’로 판단한다.

3) 기준금액 산출

피심인이 운영하는 쇼핑몰(,) 및 쇼핑앱( )의 회원정보가 모두 유출되었으므로, 해당 서비스들의 직전 3개 사업년도의 연평균 매출액 천원에 ‘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				

* 자료출처 : 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

<보호법 시행령 [별표 1] 2. 가. 1)에 따른 과징금 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

피심인이 '이용자의 개인정보를 유출한 경우로서 안전성 확보에 필요한 조치를 하지 않은 행위('21.4.9.~'21.10.22.)'의 위반기간이 과징금 부과기준 제6조와 제7조에 따라 1년 이내의 '단기 위반행위'에 해당하므로 기준금액을 유지하고, 최근 3년간 보호법에 의한 과징금 처분을 받은 적이 없으므로 기준금액의 100분의 50에 해당하는 금액인 천원을 감경한다.

라. 추가적 가중 및 감경

과징금 부과기준 제8조는 사업자의 위반행위 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중 · 감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

가중 사유는 없으며, 개인정보 유출 사실을 자진 신고한 점, 조사에 적극 협력한 점을 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 제48조의11제1항·제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 천원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금*
973,368천원	필수적 가중 없음 필수적 감경 (50%, 천원)	추가적 가중 없음 추가적 감경 (20%, 천원)	
	→ 천원	→ 천원	

* 최종 과징금 산출액이 1억원 미만은 십만원 미만 절사, 1억원 이상은 백만원 미만 절사함

2. 과태료 부과

피심인의 보호법 제21조제1항, 제29조 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제4호·제6호, 같은 법 시행령 제63조의〔별표2〕'과태료 부과기준' 및 「개인정보 보호법 위반에 대한 과태료 부과기준」(2021. 1. 27. 개인정보보호위원회 의결, 이하 '과태료 부과지침'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 600만원을 각각 적용한다.

< 「보호법」 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
마. **법 제21조제1항**·제39조의6(제39조의14에 따라 준용되는 경우를 포함한다)을 **위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우**	법 제75조 제2항제4호	600	1,200	2,400
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 부과지침 제8조(과태료 가중기준)에 따라, 안전성 확보에 필요한 조치를 하지 않은 행위에 대하여 ▲제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상인 경우 및 위반 기간이 3개월 이상인 경우로 기준금액의 20%를 가중하며, 개인정보 파기 등 필요한 조치를 하지 않은 행위에 대하여 ▲위반 기간이 3개월 이상인 경우로 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 과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점을 고려하여 기준금액의 50%를 각각 감경한다.

다. 최종 과태료

피심인의 보호법 제21조제1항, 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 780만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보의 파기	600만원	60만원	300만원	**360만원**
안전조치의무 위반 (접근통제, 접속기록)	600만원	120만원	300만원	**420만원**
계	-	-	-	**780만원**

3. 결과 공표

보호법 제66조제1항 및 '개인정보보호위원회 처분결과 공표기준(2020. 11. 18. 개인정보보호위원회 의결)' 제2조(공표요건)에 따르면 피심인의 위반행위는 보호법 제75조제2항 각 호에 해당하는 위반행위 2개 이상 한 경우(제4호)에 해당하므로 보호법 제66조제1항에 따라 피심인에 대한 과태료 부과 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표				
위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	위반조항	위반내용	처분일자	처분내용
	법 제21조제1항	개인정보 미파기	2022. 7. 13.	과태료 부과 780만원
	법 제29조	안전조치의무 위반		

Ⅴ. 결론

피심인의 보호법 제21조제1항, 제29조 위반행위에 대하여 같은 법 제39조의15(과징금 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항제4호·제6호 및 제66조(결과의 공표)제1항에 따라 과징금, 과태료 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.

2022년 7월 13일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(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)