

방 송 통 신 위 원 회

심의 · 의결

안건번호 제2019 - 57 - 302호

안 건 명 통신사 영업점 등 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2019. 11. 22.

주 문

1. 피심인은 개인정보를 처리할 때에는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.
2. 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.
3. 피심인에 대하여 다음과 같이 과징금 및 과태료를 부과한다.



- 가. 과정금 : 1,852,000,000원
- 나. 과태료 : 10,000,000원
- 다. 납부기한 : 고지서에 명시된 납부기한 이내
- 라. 납부장소 : 한국은행 국고수납 대리점
- 마. 과태료를 내지 않으면 질서위반행위규제법 제24조, 제52조, 제53조제1항 및 제54조에 따라 불이익이 부과될 수 있음

이 유

I. 기초 사실

(이하 「피심인」이라 한다)는 영리를 목적으로 온라인 쇼핑몰 서비스를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 「정보통신망법」이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수(‘18.11.14. 기준)

< 피심인의 최근 3년간 매출액 현황 >

(단위 : 백만원)

구 분	2015년	2016년	2017년	평 균
관련 매출액				

※ 자료 출처 : 피심인이 제출한 자료

II. 사실조사 결과



1. 조사 대상

방송통신위원회는 피심인이 운영 중인 웹사이트의 이벤트페이지에 모바일 웹을 통하여 로그인 시, 타인의 주문정보 접근이 가능하게 되었으며 이용자가 특정 페이지(마이페이지, 구매정보)에 접속하면서 타인의 개인정보 20건이 권한 없는 타인에게 노출되었다는 피심인의 신고(2018. 11. 2.)를 접수하였다.

※ 유출인지 : 고객 온라인 게시판을 통해 모바일 웹에서 타인으로 로그인 되었다는 민원이 접수되어 인지함

이에, 방송통신위원회는 한국인터넷진흥원과 함께 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2018. 11. 14.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 웹페이지 및 모바일 앱()으로 온라인 쇼핑몰 서비스를 제공하면서 2018. 11. 14. 기준으로 건의 회원정보를 보유하고 있다.

< 피심인의 개인정보 수집 현황 >

구 분	항 목	수집일	건수
유효회원	[필수] 이름, 생년월일, 이메일, 비밀번호, 휴대전화번호 [선택] 성별, 주소		건
휴면회원	상동		건
계			건

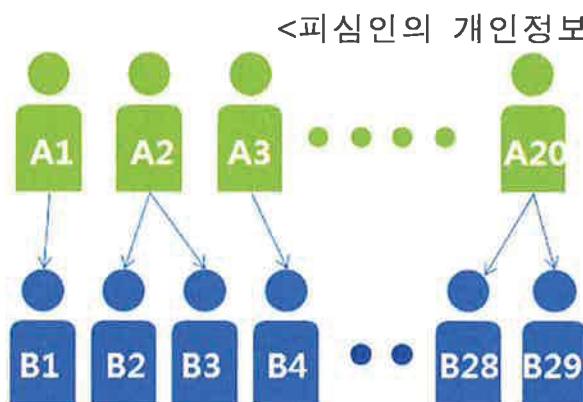


나. 개인정보 유출 규모 및 경로

1) 개인정보 유출규모

피싱인이 ‘온라인 전자상거래’ 서비스를 운영하면서 수집한 회원의 개인정보 약 20건*이 타인에게 노출되었다.

* 20명의 이용자 개인정보가 해당 페이지에 로그인한 이용자 29명에게 노출됨



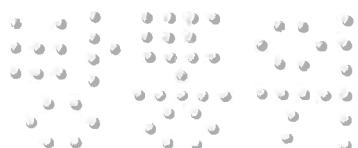
2018.11.1. ‘
이벤트 시 모바일웹(Web)으로 접속한
20명의 이용자 개인정보가 같은
시간대 해당 페이지에 로그인한
29명의 이용자에게 노출됨

< 피싱인의 개인정보 유출현황 >

구 분	유 출 항 목	건 수
회원	이름, 이메일, 휴대폰번호, 배송지 주소	20건

2) 유출 경로

피싱인이 2018. 11. 1. 00:00에 새로운 캐시 정책을 적용한
‘
이벤트 페이지
’
를 오픈하면
서 캐시 설정 오류로 인하여 타인의 캐시 데이터를 받은 이용자가 특정 페이지
(마이페이지, 구매정보)에 접속하면서 타인의 개인정보 총 20건이 노출되었다.

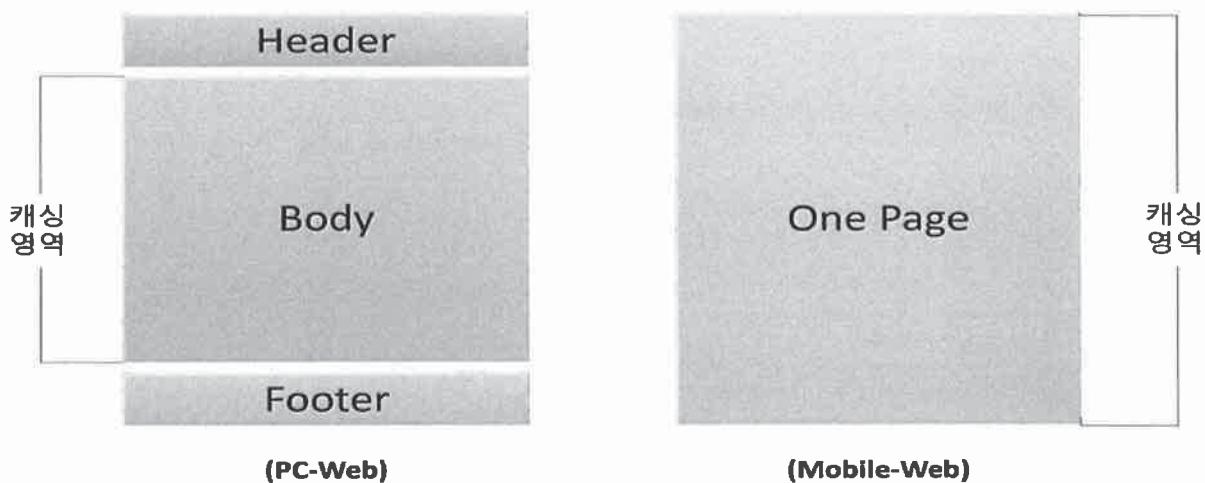


3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출{정보통신망법 제28조(개인정보의 보호조치) 중 개인정보 유·노출 방지조치}되지 않도록 조치를 취하지 않은 행위

피심인은 2018. 10. 30. ‘이벤트대비 서버 폭주에 따른 이용자 접속 지연 해결을 위해 개발부서에 새로운 캐시(Cache)정책 배포를 요청하였고, 이를 개선하기 위해 Nginx¹⁾(‘엔진엑스’라 읽는다) 중 캐싱을 통한 Fast CGI²⁾ 기능을 Mobile Web 부분에 적용(2018. 10. 31. 22:00)하였다. 2018. 11. 1. 00:00 이벤트 페이지를 오픈하였으나, 정상적인 캐시 설정에는 웹페이지 정보(페이지 HTML)만 저장해야 하는데 새로 배포된 캐시 설정에는 이용자의 쿠키정보(자동로그인 토큰)까지 저장되어 캐시 저장 후 1분 이내에 이벤트 페이지 접속 시 타인의 캐시 데이터를 받은 이용자(29명)가 특정 페이지(마이페이지, 구매정보)에 접속하면서 타인의 정보(20명)가 노출되도록 한 사실이 있다.

<피심인이 ‘이벤트 대비 적용한 캐시 정책>



1) Nginx : 오픈 소스 기반 웹 서버 프로그램으로 Fastcgi를 이용한 Cache기능을 기본적으로 제공한다. 웹 서버 프로그램으로는 아파치(Apache) 웹서버, 구글 웹서버 등이 있다.

2) Fast CGI : 하나의 프로세스가 다중 CGI 요청을 처리하도록 하여 속도를 향상시킨 웹 서버 플러그 인 프로그램으로, 모든 프로세스 요청이 하나의 프로세스를 공유하기 때문에 많은 프로그램 명령이 절약되어 처리 속도가 빠르다.



나. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2019. 2. 20. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 3. 4. 의견을 제출하였다.

III. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 “정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령이 정하는 기준에 따라 ‘개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)’을 하여야 한다.”라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)’를 하여야 한다.”고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 ‘고시’) 제4조제9항은 “정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.”라고 규정하고 있다.

‘고시 해설서’는 고시 제4조제9항에 대해 “정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보



안 기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 한다.”라고 해설하고 있다.

나. 정보통신망법 제64조제3항은 “방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출(정보통신망법 제28조(개인정보의 보호조치) 중 개인정보 유·노출 방지조치)되지 않도록 조치를 취하지 않은 행위

고시 제4조제9항의 입법 목적은 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 여러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성하는 등 보안대책을 마련하여야 한다는 것이다.

피심인이 PC web 이벤트 페이지에 대해서는 서버에서 Json을 캐싱하도록 설정하였으나(Html의 body부분만 캐싱), mobile web 이벤트 페이지는 전체를 캐싱하도록 설정하였고, 이 과정에서 이용자를 식별할 수 있는 쿠키 값(wmp_web_token)마저 캐싱되어, 캐시 저장 후 1분 이내에 이벤트 페이지 접속 시 타인의 캐시 데이터를 받은 이용자(29명)가 특정 페이지(마이페이지, 구매정보)에 접속하면서 타인의 정보(20명, 항목 : 이름, 이메일, 휴대폰번호, 배송지 주소)가 열람권한이 없는 자에게 공개되도록 한 행위는, 정보통신망법 제28조제1항 제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.



<피심인의 노출 사고 시나리오>

- ① 다수의 이용자가 자동 로그인 체크하여 로그인, 이 때 쿠키(로그인쿠키)와 (자동 로그인 쿠키)가 생성
- ② 이벤트 페이지 전체를 캐시 설정하여 이용자의 (로그인쿠키)와 (자동 로그인 쿠키)이 캐싱 데이터에 저장됨
- ③ ①의 과정을 거친 사용자들이 브라우저를 닫고 새롭게 브라우저를 연 후 이벤트 페이지 URL에 직접 접근
- ④ 특정 시간(캐시 저장 후 1분 이내)내 이벤트 페이지를 재 접속 시 타인의 쿠키가 저장된 캐시 정보를 반환 처리
- ⑤ 타인의 캐시 데이터를 받은 이용자가 개인정보 또는 구매 정보 등 특정 페이지 접속 시 타인의 정보가 노출됨

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②5호	취급 중인 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하지 아니한 행위(고시§4⑨)

IV. 시정조치 명령

1. 시정명령

피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.



2. 시정명령 이행결과의 보고

피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

V. 과징금 부과

피심인은 정보통신망법 제64조의3제1항제6호에 따라 이용자의 개인정보가 분실·유출된 경우로서 개인정보 보호조치(제28조제1항)를 하지 않은 경우에 해당하여, 위반행위와 관련한 매출액의 100분의 3 이하의 과징금을 부과할 수 있다.

피심인의 경우, 직원 실수로 인하여 일시적(약 34시간)으로 타인의 개인정보가 소규모 노출(20건)된 사안이나, 최근 3년간 유사한 위반행위로 처분(의 결, 과태료처분)을 받았음에도 유출사고가 재발한 2회 위반 사업자라는 점을 고려하여 과징금을 부과한다.

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조의3 제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 [별표 8] (과징금의 산정 기준과 산정절차) 및 ‘개인정보보호 법규 위반에 대한 과징금 부과기준(방송통신위원회 고시 제2015-30호, 이하 ‘과징금 부과기준’이라 한다)’ 따라 다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금 상한액은 같은 법 제



64조3의제1항, 같은 법 시행령 제69조의2에 따라 위반행위와 관련된 정보통신서비스의 직전 3개년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

과징금 부과기준 제5조제1항은, 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 정보통신망법 제28조제1항에 따른 기술적·관리적 보호조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따를 때, ▲피심인의 행위가 고의성이 없고 단순 과실로 보이는 점을 고려하면 피심인에게 중과실이 있다고 보기 어렵다.

2) 중대성의 판단

과징금 부과기준 제5조제2항은, 위반 정보통신서비스 제공자등에게 고의 · 중과실이 없으면 위반행위의 중대성을 보통 위반행위로 판단한다고 규정하고 있다.

이에 따를 때, 피심인의 고의·중과실이 없으므로 ‘보통 위반행위’로 판단한다.

3) 기준금액 산출

피심인은 위반행위와 관련된 매출액에 대해 ‘개인정보 노출사건으로 인하여 직접 영향을 받은 서비스는 ’ 이벤트 모바일 웹부문에 해당하고 이외에 간접적으로 영향을 받은 서비스를 특별히 산정하기 어려워 위반행위



와 관련된 정보통신서비스 매출액은 ‘이벤트 모바일 웹부문 매출액으로 한정해야 하나, 해당 이벤트는 ‘18년에 처음 실시된 서비스로 ‘18년 직전 3개 사업연도의 매출액이 없어 매출액 산정이 곤란한 경우에 해당, 과징금을 부과하더라도 정액 과징금으로 부과하는 것이 타당’하다는 의견을 제출하였다,

‘이벤트는 새로운 사업이 아닌 전체 쇼핑몰 사업의 일환으로 진행되었고 서비스 범위도 동일하여 위반행위 관련 매출액을 ‘이벤트로 한정하여 산정하는 것은 부적절하므로, 위 의견을 수용하지 않았다.

이에 따라 피심인의 위반행위와 관련된 매출액을 위반행위와 관련된 매출로 하고, 위반행위와 관련된 직전 3개 사업연도의 연평균 매출액 천원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 ‘보통 위반행위’의 부과기준을 1천분의 15를 적용하여 기준금액을 원으로 한다.

<정보통신망법 시행령 [별표 8] 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 이내 ‘단기 위반행위’에 해당하므로 기준금액을 유지하고,

최근 3년간 정보통신망법 제64조의3제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 원을 감경한다.



라. 추가적 가중 및 감경

과징금 부과기준 제8조에 따라 위반행위의 주도 여부, 위반행위에 대한 조사의 협조 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따를 때, 피심인이 ▲개인정보 유출사실을 자진 신고한 점, ▲조사에 성실히 협조한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 30에 해당하는 원을 감경한다.

2. 과징금의 결정

피심인의 정보통신망법 제28조(개인정보의 보호조치) 위반행위에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2 [별표 8] 2. 가. 1) (과징금의 산정기준과 산정절차) 및 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 원이나, 최종 과징금 산출액이 1억원 이상에 해당하여 백만원 미만을 절사한 1,852,000,000원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금*
천원	필수적 가중 없음 필수적 감경 (50%, 천원)	추가적 가중 없음 추가적 감경 (30%, 천원)	1,852백만원
	→ 천원	→ 천원	

* '전기통신사업법 금지행위 위반에 대한 과징금 산정 실무요령'에 따라 최종 과징금 산출액이 1억원 미만은 십만원 미만 절사, 1억원 이상은 백만원 미만 절사함

VI. 과태료 부과



피침인의 정보통신망법 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표9] 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피침인은 최근 3년간 같은 위반행위로 과태료 처분('17. 10. 12.)을 받은 사실이 있으므로 2회 위반에 해당하는 2,000만원을 적용한다.

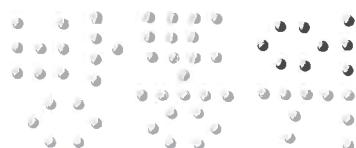
< 위반 횟수별 과태료 금액 >

위 반 사 항	근거법령	위 반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조 제1항제3호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) (과태료의 가중) 과태료 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보제공 등 조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 가중할 수 있다고 규정하고 있다.

그러나 피침인의 정보통신망법 제28조제1항 위반 행위에 대해서 특별히 해당 사항이 없으므로 과태료를 가중하지 않는다.



2) (과태료의 감경) 과태료 부과지침 제7조는 ▲당사자 환경, ▲사업규모와 자금사정, ▲개인(위치)정보보호 노력정도, ▲조사협조 및 자진시정, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 감경할 수 있다고 규정하고 있다.

이에 따라 피심인의 정보통신망법 제28조제1항 위반 행위에 대해 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정 완료한 점을 고려하여 기준 금액의 50%인 1,000만원을 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①2호	2,000만원	없음	1,000만원	1,000만원
계				1,000만원

다. 최종 과태료

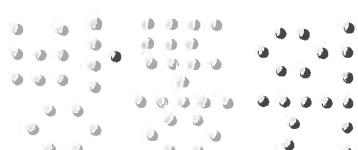
이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 1,000만원의 과태료를 부과한다.

< 위반행위별 과징금 · 과태료와 시정명령 >

위반 유형	과징금	과태료	시정명령	계
기술적·관리적 보호조치 §28①2호	185,200만원	1,000만원	O	186,200만원

VII. 고 발

피심인의 위반행위는 정보통신망법 제28조제1항제2호부터 제5호까지의 규정에



따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 유출한 경우이므로 같은 법 제64조의3제1항제6호에 해당하는 행위가 있다고 인정된다. 이에 피심인을 같은 법 제73조(벌칙) 및 제69조의2(고발) 규정에 따라 수사기관에 고발한다.

VIII. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조제1항제3호(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 방송통신위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 방송통신위원회의 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.

이에 주문과 같이 의결한다.



2019년 11월 22일

위 원 장

한 상 혁



부위원장

김 석 진



위 원

허 우



위 원

표 철 수



위 원

김 창 룡

