방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 35 - 391호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2018. 7. 11.

주 문

1. 피심인은 본인확인기관으로 지정받은 바 없고, 법령·고시에서 주민등록번호 수집·이용을 허용하는 경우에도 해당하지 아니하므로 이용자의 주민등록번호를 수집·이용하여서는 아니 된다.

2. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

가. 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여할 것

나. 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을

제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것

다. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리할 것

3. 피심인은 제1항부터 제2항까지의 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.

4. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금　　액 : 25,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

라. 과태료를 내지 않으면 질서위반행위규제법 제24조, 제52조, 제53조제1항 및 제54조에 따라 불이익이 부과될 수 있음

이　　유

Ⅰ. 기초 사실

피심인은 영리를 목적으로 홈페이지(　　등)를 통해 여행상품 예약 등의 서비스를 제공하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법' 이라 한다) 제2조 제1항 제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

〈참고 1〉 피심인의 일반현황

대표이사	설립일자	자본금	주요서비스	종업원 수

〈참고 2〉 피심인의 최근 3년간 매출액 현황

(단위 : 백만원)

구 분	2015년	2016년	2017년	평 균
매출액				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

경찰청이 ‘ ’ 해커를 추가 조사하는 과정에서 피심인의 개인정보가 유출되었다는 내용을 방송통신위원회에 알려옴('18.1.24.)에 따라, 방송통신위원회는 피심인을 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2018.3.8.~2018.3.9.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 ‘여행상품 예약’ 서비스 홈페이지 ( ) 및 패밀리사이트 ( )를 운영하면서 홈페이지 회원가입 및 전화상담 예약 등으로 2018. 3. 8. 기준으로

22,584건의 개인정보를 수집·보관하고 있다.

〈참고 3〉 피심인의 개인정보 수집 현황

구 분	항 목	수집일	건수
홈페이지 회원	아이디, 비밀번호, 이름, 영문이름, 생년월일, 주소, 휴대전화번호 등	'10. 8. 30.~	3,469건
여행상품 예약	이름, 이메일, 휴대전화번호 등	'14. 1. 2. ~	19,115건
계			22,584건

나. 개인정보 유출 규모 및 경로

(1) 개인정보 유출규모

피심인이 운영하는 개인정보처리시스템(DB)에 보관되어 있던 (
)*에서 2001.4월~2009.5월 사이에 수집한 201,686건의 개인정보가 유출되었다.

* 피심인은 2009년말 여행업을 준비하는 과정에서 에서 운영하던 DB서버 및 웹서버를 무상으로 인수 했다고 진술함

〈참고 4〉 피심인의 유출 현황

구 분	유 출 항 목	건 수
DB 개인정보	아이디,비밀번호,성명,주민등록번호,주소,집전화번호, 휴대전화번호,이메일,여권번호	201,686건**

** 경찰청 분석 결과를 기준으로 개인정보 유출 건수를 산출함

(2) 유출 경로

피심인의 개인정보 유출시기 및 유출경로는 확인이 어려우며, 숙박앱 '
' 를 해킹한 해커가 알 수 없는 방법으로 해킹해 개인정보를 유출한 것으로 추정된다.

(3) 유출 신고

피심인은 2018.3.28. 한국인터넷진흥원으로부터 연락을 받고 2018.3.29. 개인정보보호 포털(www.i-privacy.kr)에 개인정보 유출을 신고하였다.

피심인은 유출정보가 피심인의 고객이 아닌 2009년말 에서 운영하던 DB서버 및 웹서버에 있던 개인 정보인 관계로 이용자 유출통보에 대한 내부회의를 통해 보내는 방식과 내용 등을 검토하고 2018.5.11. 이용자에게 이메일로 통보하였다.

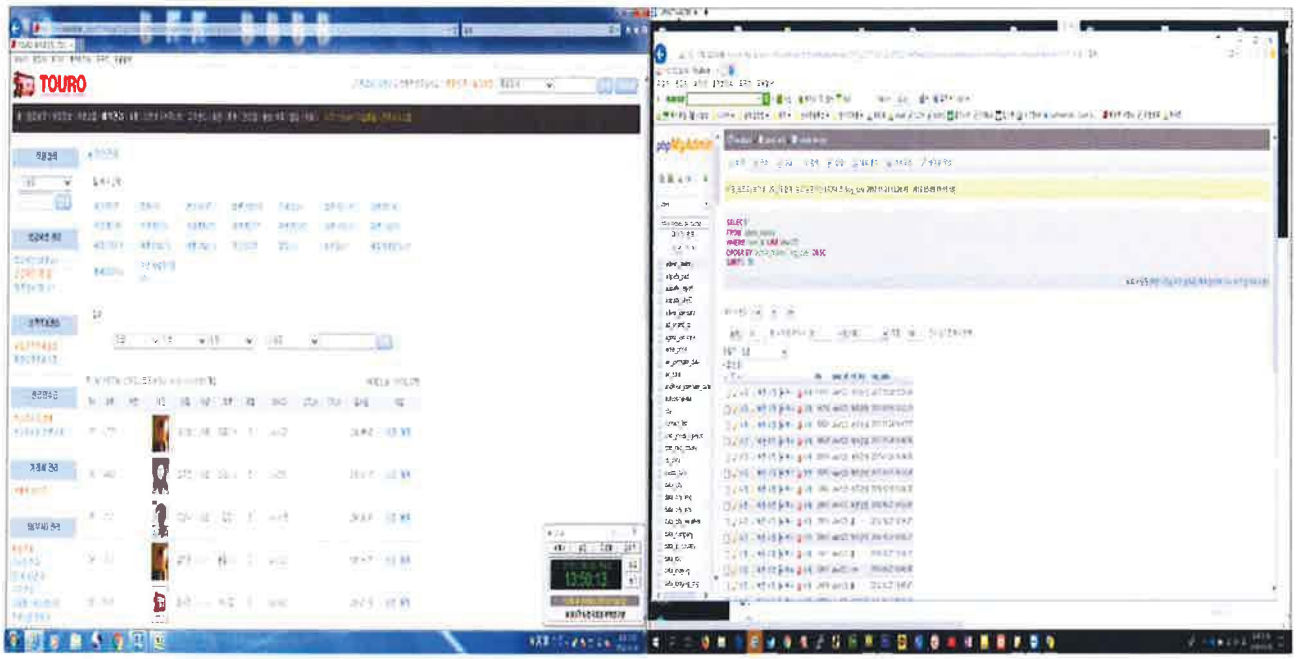
3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 이용자의 주민등록번호를 파기{정보통신망법 제23조의2(주민등록번호의 사용 제한)}**하지 않은 행위**

피심인은 개인정보처리시스템 내 총 3개 테이블( ) 내에 보유하고 있던 주민등록번호 약 145,159여건을 경찰청 조사를 받고 2017.7.13. 삭제 조치 전까지 저장·관리한 사실이 있다.

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**를 소홀히 한 행위**

1) (접근권한 최소 부여) 피심인은 사업운영 초기 자문을 받기 위해 개인정보처리시스템의 관리자페이지( )에 대한 접근권한을 외부인 엄○○(근무한 적 없음)에게 최고레벨 권한을 부여(2010.6.25.)하였고, 말소하지 않은 엄○○ 계정( )을 직원들이 공유해 2017.11.24.까지 접속한 사실이 있다.



2) (침입탐지시스템 설치·운영) 피심인은 2018. 3. 8. 현재 운영 중인 개인정보처리시스템에 접속한 IP 등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는 기능을 포함한 침입탐지 시스템을 설치·운영하지 않은 사실이 있다.

다. 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

피심인은 개인정보취급자가 개인정보처리시스템(DB)에 접속한 처리일시, 처리내역 등 접속기록을 보존·관리하지 아니하였고, 접속기록이 위·변조되지 않도록 별도의 물리적인 저장장치에 보관하고 정기적인 백업을 수행하지 않았으며, DB 및 관리자페이지 접속기록을 월1회 이상 정기적으로 확인·감독한 사실이 없다.

라. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 4. 26. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 5. 16. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제23조의2제1항은 "정보통신서비스 제공자는 '제23조의3에 따라 본인확인기관으로 지정받은 경우(제1호)', '법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우(제2호)', '영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우(제3호)' 에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다." 라고 규정하고 있다.

부칙 제2조제1항은 "주민등록번호 수집·이용 제한에 관한 경과조치로 이 법 시행 당시 주민등록번호를 사용한 회원가입 방법을 제공하고 있는 정보통신서비스 제공자는 이 법 시행일부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 한다. 다만, 제23조의2제1항 각 호의 어느 하나에 해당하는 경우는 제외한다." 고 규정하고 있고, 제2항은 "제1항에 따른 기간 이내에 보유하고 있는 주민등록번호를 파기하지 아니한 경우에는 제23조의2제1항의 개정규정을 위반한 것으로 본다." 라고 규정하고 있다.

나. 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 유출 시도를 탐지하는 침입탐지시스템 등 접근 통제장치의 설치·운영(제2호)', '접속기록의 위조·변조 방지를 위한 조치(제3호)' 를 하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 " 개인정보처리시스템 "이라 한다)에 대한 접근권한의 부여·변경·

말소 등에 관한 기준의 수립·시행(제1호), 개인정보처리시스템에 대한 침입차단 시스템 및 침입탐지시스템의 설치·운영(제2호)' 하여야 한다." 고 규정하고 있고, 제3항은 "접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 확인·감독(제1호)', '개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관(제2호)' 의 조치를 하여야 한다." 라고 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' 라고 함) 제4조제1항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다." 고 규정하고 있으며, 제5항은 "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 있다.

고시 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다." 라고 규정하고 있다.

다. 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. 이용자의 주민등록번호를 파기{정보통신망법 제23조의2(주민등록번호의 사용 제한)}**하지 않은 행위**

정보통신망법 제23조의2제1항은 본인확인기관이거나 법령이나 고시에서 주민등록번호의 수집·이용을 허용하는 경우가 아니면 주민등록번호를 수집·이용할 수 없도록 규정하고 있으며, 2012.2.17. 시행한 정보통신망법 부칙 제2조에 따라 기존에 보유하고 있는 주민등록번호도 2014년 8월 이전까지 삭제하여야 한다.

피심인이 개인정보처리시스템(DB)에서 보유하고 있던 주민등록번호를 2014.8.17. 까지 파기하지 아니한 행위는 정보통신망법 제23조의2제1항, 부칙 제2조제2항을 위반한 것이다.

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**를 소홀히 한 행위**

1) (접근권한 최소 부여) 고시 제4조제1항의 입법 목적은 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위해 필요한 최소한의 인원에게 부여하여야 하고 특히, 개인정보처리시스템의 데이터베이스(DB)에 직접 접속은 데이터베이스 운영·관리자에 한정하는 등의 보호조치를 적용할 필요가 있으며, 개인정보처리시스템에 열람, 수정, 다운로드 등 본인 이외의 개인정보에 대한 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여하여야 한다는 것이다.

피심인이 개인정보취급자가 아닌 외부인에게 최고레벨 관리자 권한을 부여해 사용하도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제1항을 위반한 것이다.

2) (침입탐지시스템 설치·운영) 고시 제4조제5항의 입법 목적은 '정보통신망을 통한 불법적인 접근 및 침해사고 방지'인 바, 그 내용은 첫째 침입차단 및 침입탐

지 기능을 포함한 시스템의 '설치' 의무이고, 둘째 침입차단 및 침입탐지 기능을 포함한 시스템의 '운영' 의무이다.

먼저 시스템 '설치' 의무에 대하여 살펴보면, 정보통신서비스 제공자등은 ①접속권한을 IP주소 등으로 제한하여 비인가 접근을 '차단'하는 기능(침입차단 기능)과 함께 ②개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법유출 시도를 '탐지'하는 기능(침입탐지기능)을 보유한 시스템을 설치하여야 한다.

피심인이 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 침입탐지시스템을 설치·운영하지 않은 행위는 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항 제2호, 고시 제4조제5항제2호를 위반한 것이다.

다. 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

고시 제5조제1항의 입법 목적은 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인을 위해 식별자(개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 ID 등), 접속일시(개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시:분:초)), 접속지(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP주소 등), 수행업무(개인정보처리시스템에서 개인정보취급자가 처리(개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위)한 내용을 알 수 있는 정보) 등을 포함하는 접속기록을 최소 6개월 이상 보존·관리하여야 한다는 것이다.

피심인이 개인정보취급자의 개인정보처리시스템(DB) 접속기록을 월1회 이상 정기적으로 확인·감독을 하지 아니하고, 최소 6개월 이상 접속기록을 보존·관리하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항

제1호, 고시 제5조제1항을 위반한 것이다.

〈참고 5〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	주민등록번호	§23의2①		법적 근거없이 이용자의 주민등록번호를 수집·이용한 행위
	접근통제	§28①2호	§15②1호	개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여하지 아니한 행위(고시§4①)
	접근통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치하지 아니한 행위(고시§4⑤)
	접속기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 아니한 행위(고시§5①)

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 본인확인기관으로 지정받은 바 없고, 법령·고시에서 주민등록번호 수집·이용을 허용하는 경우에도 해당하지 아니하므로 이용자의 주민등록번호를 수집·이용하여서는 아니 된다.

나. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여할 것

2) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리할 것

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.

3. 과태료 부과

피심인의 정보통신망법 제23조의2(주민등록번호 사용 제한)제1항, 제28조(개인정보의 보호조치)제1항 위반에 대한 과태료는 같은 법 제76조제1항제2호·제3호, 같은 법 시행령 제74조의 〔별표9〕 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」 (이하 '과태료 부과 등 처리지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과 등 처리지침 제7조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하므로 1회 위반 과태료인 1,000만원을 각 적용한다.

〈참고 6〉 위반 횟수별 과태료 금액

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
다. 법 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 않은 경우(법 제67조에 따라 준용되는 경우를 포함한다)	법 제76조제1항 제2호	1,000	2,000	3,000
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

과태료 부과 등 처리지침 제9조는 ▲위반행위가 2개 이상인 경우, ▲위반행위가 2개 이상에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기·정도, 사회·경제적 파급 효과 등을 고려하여 과태료를 가중 부과할 필요가 있다고 인정되는 경우에는, 과태료 부과 등 처리지침 제7조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

이에 따라 피심인의 정보통신망법 제28조제1항 위반 행위가 2개 이상인 경우에 해당하므로 기준 금액의 50%를 가중한다.

〈참고 7〉 과태료 산출내역

위반조문	기준금액	가중	감경	최종 과태료
§23의2①	1,000만원	없음	없음	**1,000만원**
§28①2·3호	1,000만원	500만원	없음	**1,500만원**
계				**2,500만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제23조의2제1항, 제28조제1항 위반행위에 대해 2,500만원의 과태료를 부과한다.

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조(과태료)제1항제2호의3·제3호·제4호에 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.

위 원 장　　이 효 성　(인)

부위원장　　허　　욱　(인)

위　　원　　김 석 진　(인)

위 원 표 철 수 (인)

위 원 고 삼 석 (인)