방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 35 - 390호

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

다. 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화할 것

2. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

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(　　)를 통해 국내외여행 예약 서비스를 제공하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법' 이라 한다) 제2조제1항제3호에 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				
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.~9.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 ‘국내외 여행상품 예약’ 서비스를 운영하면서 2018. 3. 9. 기준으로 137,750건의 회원정보를 보유하고 있다.

〈참고 3〉 피심인의 개인정보 수집 현황

구 분	항 목	수집일	건수
회원정보	이름,아이디,비밀번호,닉네임,이메일,휴대전화번호	'14. 3. ~	137,750건

나. 개인정보 유출 규모 및 경로

(1) 개인정보 유출규모

피심인이 운영하는 홈페이지(　　)의 회원정보 124,546건이 유출되었다.

〈참고 4〉 피심인의 유출 현황

구 분	유 출 항 목	건 수
회원정보	아이디,비밀번호(암호화),주민등록번호(암호화)*,이름,이메일,집전화번호,직장주소,직장전화번호,팩스번호,휴대전화번호,집주소,성별,생년월일	124,546건

* 현장조사 시 주민등록번호는 파기되어 저장되어 있지 않음을 확인

(2) 유출 경로

숙박앱 '　　'를 해킹한 해커가 알 수 없는 방법으로 124,546건의 개인정보를 유출한 것으로 추정된다.

(3) 유출 신고

피심인은 2018.2.13. 서울전파관리소로부터 연락을 받은 후 유출 사고를 인지하였으며, 2018.2.14. 개인정보보호 포털(www.i-privacy.kr)에 개인정보 유출 사실을 신고하고 이용자에게 메일로 통보하였다. 또한 같은 날 유출 사실을 홈페이지에 공지하였다.

3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

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

피심인은 2018. 3. 8. 현재 개인정보처리시스템인 관리자 페이지(

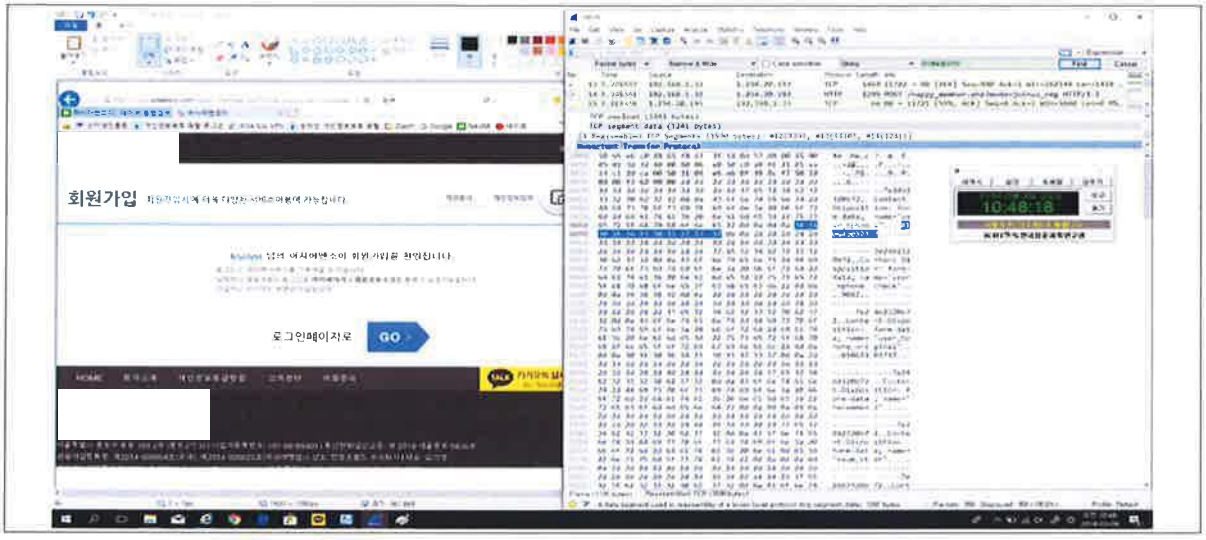
)에 대한 접근권한을 하나의 계정(admin)으로 8명의 개인정보취급자가 사용하게 한 사실이 있다.

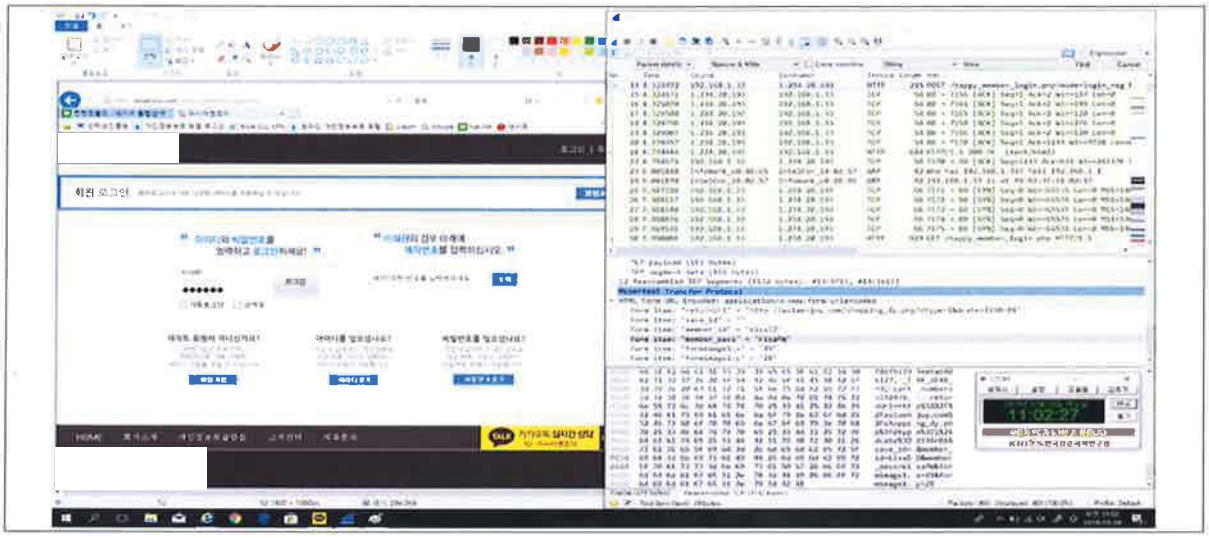
나. 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

피심인은 개인정보취급자가 개인정보처리시스템에 접속한 처리일시, 처리내역 등 접속기록을 최소 6개월 이상 보존·관리하여야 하나 DB 접속기록은 존재하지 않으며, 접속기록을 월1회 이상 정기적으로 확인·감독한 사실이 없다.

다. 암호화기술 등을 이용한 보안조치{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

피심인은 홈페이지 회원가입 및 로그인 시 이용자의 PC에서 개인정보처리시스템으로 개인정보(아이디, 비밀번호, 휴대폰번호)를 전송하는 구간에 대하여 암호화 조치를 하지 않은 사실이 있다.





라. 서비스를 이용하지 않는 이용자의 개인정보를 파기 또는 별도로 저장·관리하지 않은 행위{정보통신망법 제29조(개인정보의 파기) 중 개인정보 유효기간제}

피심인은 운영 중인 홈페이지를 이용하는 이용자로부터 이름, 이메일, 닉네임, 비밀번호, 휴대 전화번호 등 을 수집하여 2018.3.8. 현재 137,750명의 이용자 정보를 피심인의 개인정보처리시스템 내 회원DB에 저장・관리하고 있다. 피심인은 2017. 3. 8. 이후 서비스를 이용한 사실이 없어 1년 동안 서비스를 이용하지 않은 이용자 126,909명의 개인정보를 파기하지 않았으며, 서비스를 이용하고 있는 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

마. 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. 14. 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)', '접속기록의 위조·변조 방지를 위한 조치(제3호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)'를 하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템(개인정보처리시스템)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)'을 하여야 한다." 라고 규정하고 있다.

같은 법 시행령 제15조제3항은 "접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)' 하여야 한다." 라고 규정하고 있으며, 제4항은 "개인정보가 안전하게 저장·전송될 수 있도록 '정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송수신하는 경우 보안서버 구축 등의 조치' (제3호)를 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'라 한다) 제4조제1항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다." 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.

고시 제6조제3항은 "이용자의 개인정보 및 인증정보를 송수신할 때는 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하거나(제1호), 웹서버에 암호화 응용프로그램을 설치하여(제2호) 전송하는 정보를 암호화하여 송수신하는 기능을 갖추어야 한다." 라고 규정하고 있다.

나. 정보통신망법 제29조제2항은 "정보통신서비스 제공자등은 정보통신서비스를 1년의 기간동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제16조제2항은 "정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제29조제2항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다." 라고 규정하고 있다.

다. 정보통신망법 제64조제3항은 "과학기술정보통신부장관 또는 방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반 한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다." 라고 규정하고 있다.

2. 위법성 판단

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

고시 제4조제1항의 입법 목적은 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위해 필요한 최소한의 인원에게 부여하여야 하며 특히, 개인정보처리시스템의 데이터베이스(DB)에 직접 접속은 데이터베이스 운영·관리자에 한정하는 등의 보호조치를 적용할 필요가 있으며, 개인정보

처리시스템에 열람, 수정, 다운로드 등 본인 이외의 개인정보에 대한 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여하여야 한다는 것이다.

피심인이 개인정보취급자 8명에게 전체 권한이 있는 하나의 계정을 사용하도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제1항을 위반한 것이다.

나. 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 IP 주소 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 접속일시·처리내역 등 접속기록을 작성하여 월1회 이상 이를 확인·감독하지 않았으며 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 개인정보처리시스템의 접속기록(로그기록)을 보존·관리하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

다. 암호화기술 등을 이용한 보안조치{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

고시 제6조제3항의 입법 목적은 정보통신서비스 제공자등은 이용자의 성명, 연락처 등의 개인정보를 정보통신망을 통해 인터넷 구간으로 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 하며, SSL(Secure Sockets Layer)인증서를 이용한 보안서버는 별도의 보안 프로그램 설치 없이, 웹서버에 설치된 SSL 인증서를 통해 개인정보를 암호화하여 전송하는 방식이며, 응용프로그램을 이용한 보안서버는 웹서버에 접속하여 보안 프로그램을 설치하여 이를 통해 개인정보를 암호화 전송하는 방식을 구축하라는 것이다.

피심인이 이용자의 PC에서 개인정보처리시스템으로 개인정보를 전송하는 구간에 대하여 암호화 전송 방식을 구축하지 않은 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제3호, 고시 제6조제3항을 위반한 것이다.

라. 서비스를 이용하지 않는 이용자의 개인정보를 파기 또는 별도로 저장·관리하지 않은 행위{정보통신망법 제29조(개인정보의 파기) 중 개인정보 유효기간제}

정보통신망법 제29조제2항의 입법 목적은 장기간 서비스를 이용하지 않고 방치되는 개인정보로 인한 이용자의 피해를 방지하고 사업자의 불필요한 개인정보 보관을 최소화하기 위해 장기 미이용자의 개인정보를 보호할 수 있는 적절한 조치가 필요하고, 온라인 서비스의 경우에는 업종별 특성을 고려하여 '서비스 이용 기록, '접속로그' 등을 기준으로 서비스 이용여부를 판단할 수 있으며, 이용자의 이해를 돕기 위해 이용약관 등을 통해 그 적용 기준에 대해 명확히 알려주는 것이 필요하다는 것이다.

피심인이 정보통신서비스를 1년의 기간 동안 이용하지 않은 이용자의 개인정보를 즉시 파기하거나 다른 이용자와 별도로 저장·관리하지 않은 행위는 정보통신망법 제29조제2항, 같은 법 시행령 제16조제2항을 위반한 것이다.

〈참고 5〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②1호	개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여하지 아니한 행위(고시§4①)
	접속 기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월 1회 이상 확인·감독하지 않고, 6개월 이상 보존·관리하지 아니한 행위 (고시§5①)
	암호화	§28①4호	§15④3호	이용자의개인정보및인증정보를송·수신할때안전한보안서버구축등의조치를통해암호화하지아니한행위(고시§6③)
	유효 기간	§29②	§16②	1년간 로그인 기록이 없는 회원의 개인정보를 파기 또는 별도 분리·보관하지 않은 행위

Ⅳ. 시정조치 명령

1. 시정명령

가. 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) 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) 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화할 것

나. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 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.

3. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항, 제29조(개인정보의 파기)제2항 위반에 대한 과태료는 같은 법 제76조제1항제3호·제4호, 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
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
더. 법 제29조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 취하지 않은 경우	법 제76조 제1항제4호	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
§28①2·3·4호	1,000만원	500만원	없음	**1,500만원**
§29②	1,000만원	없음	없음	**1,000만원**
계				**2,500만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항, 제29조제2항 위반행위에 대해 2,500만원의 과태료를 부과한다.

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조(과태료)제1항제3호·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)