방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020-28-120호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2020년 5월 19일

주 문

1. 피심인은 개인정보를 이전받으면 지체 없이 그 사실 및 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편, 서면, 모사전송, 전화 등의 방법으로 이용자에게 알려야 한다.

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. 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것

나. 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리

시스템에 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. 비밀번호는 복호화 되지 아니하도록 안전한 암호알고리즘을 이용하여 일방향 암호화하여 저장할 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 : 14,000,000원

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

1 (이하 '피심인'이라 한다.)은 가상통화 거래정보 공유 사이트 ( )를 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

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 천원)

구 분	2016년	2017년	2018년	3년 평균
전체 매출				

※

Ⅱ. 사실조사 결과

1. 조사 대상

2 방송통신위원회는 개인정보보호 포털(i-privacy.kr, KISA)에 유출신고한 사업자에 대하여 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사(2019.8.29.~30.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집 · 이용 현황

3 피심인은 가상통화 거래정보 공유 사이트( )를 운영하면서 2019.8.29. 기준 건의 이용자 정보를 수집 · 보관하고 있다.

< 개인정보 수집 · 이용 현황 >

구분	항목	수집일	건수
회원정보	이메일, 아이디, 암호화된 비밀번호		건
총 계			건

나. 개인정보 유출 관련 사실관계

(개인정보 유출 경과 및 대응)

① 미상의 해커(이하 '이 사건의 해커'라 한다)는 알 수 없는 방법으로 기 확보한 관리자 계정을 이용하여 IP(211.179.113. 등 16개)에서 '19. 8. 17. 23:04 사이트 관리자 페이지에 접속한 후

- 관리자 계정 ' '의 비밀번호를 ' '로 변경하고,
- '레이아웃 수정페이지'에서 이용자의 아이디, 비밀번호를 탈취하는 악성코드(exp.cx)를 삽입함

② 피심인 관리자는 '19. 8. 18. 00:51 이용자가 사이트에 로그인 시 느려지는 현상을 인지하고 자체 점검 중 악성코드가 삽입된 것을 발견하고 해당 코드를 삭제함

③ 이 사건의 해커는 2019.8.18 15:04, 2019.8.20. 23:39, 2019.8.21. 01:05 3회 동안 ①의 방법으로 악성코드(exp.cx)를 재차 삽입하고, 피심인 관리자는 2019.8.20. 17:56 , 2019.8.21. 00:15, 2019.8.21. 01:36 3회 동안 악성코드가 삽입된 것을 확인하고 삭제함

④ 피심인의 사이트( ) 내 악성코드가 삽입되었던 약 53시간 동안 이용자가 로그인을 시도 했던 379개 계정의 아이디, 비밀번호(평문)가 이 사건의 해커 서버(exp.cx)로 유출된 것으로 추정

⑤ 이 사건의 해커는 2019.8.21. 17:12 사이트 이용자 23개 계정의 아이디, 비밀번호(평문), 이메일을 유출함

일시		피심인의 유출인지 · 대응 내용
2019. 8. 20.		개인정보 유출 사실 인지
2019. 8. 21.	16:47	홈페이지에 개인정보 유출 사실 공지 및 수개월 이상 비밀번호를 변경하지 않는 등 취약한 이용자 계정 정지
	21:16	개인정보보호 포털에 개인정보 유출 신고

(유출 규모 및 항목)

4 - 피심인의 사이트( ) 내 악성코드가 삽입되었던 약 53시간 동안 이용자가 로그인을 시도 했던 379개 계정의 아이디, 비밀번호(평문)가 이 사건의 해커 서버(exp.cx)로 유출된 것으로 추정

5 - 이 사건의 해커는 2019.8.21. 17:12 사이트 이용자 23개 계정의 아이디, 비밀번호(평문), 이메일을 유출함

3. 개인정보의 기술적·관리적 보호조치 등 사실관계

가. 개인정보의 이전 시 이용자에게 통지를 소홀히 한 행위

6 피심인은 (사업자등록일 기준) 로부터 사이트 ( ) 및 사이트 내 이용자 정보 일체를 양수 받으면서 개인정보 이전 사실, 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편, 서면, 모사전송, 전화 등의 방법으로 이용자에게 알리지 않은 사실이 있다.

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

7 **(안전한 인증수단)** 피심인은 개인정보 취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 시 아이디, 비밀번호 외 안전한 인증 수단을 적용하지 않은 사실이 있다.

<피심인의 관리자 페이지 접속화면- ID 및 Password만으로 접속이 가능>

8 **(침입탐지 시스템 설치·운영)** 피심인은 개인정보처리시스템에 대해 AWS에서 기본으로 제공하는 AWS Security Group 방화벽 및 Cloudflare를 운영하고 있으나, 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 시스템을 설치·운영 하지 않은 사실이 있다.

다. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

9 피심인은 18,269건의 이용자 계정 비밀번호를 안전하지 않은 암호화 방식(MD5[1])으로 인코딩하여 DB에 저장한 사실이 있다.

<MD5 형식으로 저장된 이용자의 비밀번호 수>

라. 처분의 사전통지 및 의견 수렴

10 방송통신위원회는 2020. 2. 25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2020. 3. 10. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제26조제2항은 "영업양수자등은 개인정보를 이전받으면 지체 없이 그 사실 및 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다."라고 규정하고 있다.

1) MD5(Message-Digest algorithm 5) : 임의의 길이의 메시지를 입력받아 128비트짜리 고정 길이의 출력값을 내는 암호화 해시 함수, 보안강도는 80비트 미만으로 현재는 보안 관련 용도로 사용을 권장하지 않음

11 정보통신망법 시행령 제11조제1항은 "법 제26조제1항 각 호 외의 부분 및 제2항 본문에서 "대통령령으로 정하는 방법"이란 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법을 말한다. "라고 규정하고 있고, 제2항은 "정보통신서비스 제공자 등 또는 영업양수자 등이 과실 없이 이용자의 연락처를 알 수 없는 경우에 해당되어 제1항의 방법에 따라 통지할 수 없는 경우에는 인터넷 홈페이지에 최소 30일 이상 게시하여야 한다."라고 규정하고 있으며, 제3항은 "천재·지변이나 그 밖에 정당한 사유로 제2항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 둘 이상의 일반일간신문(이용자의 대부분이 특정 지역에 거주하는 경우에는 그 지역을 보급구역으로 하는 일반일간신문)에 1회 이상 공고하는 것으로 갈음할 수 있다."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 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)’를 하여야 한다.”라고 규정하고 있다.

12 정보통신망법 시행령 제15조제2항은 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)’ , ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

13 시행령 제15조제4항은 “정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 ‘비밀번호의 일방향 암호화 저장(제1호)’을 하여야 한다.” 라고 규정하고 있다.

14 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."라고 규정하고 있고, 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 있다.

15 고시 제6조제1항은 "정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다."라고 규정하고 있다.

16 '고시 해설서'는 고시 제4조제4항에 대해 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지기 때문에 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단의 적용이 필요하다고 해설하고 있으며, 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있다.

17 고시 제6조제1항에 대해 정보통신서비스 제공자등은 이용자 및 개인정보취급자 등의 비밀번호가 노출 또는 위·변조되지 않도록 개인정보처리시스템, 업무용컴퓨터, 보조저장매체 등에 개인정보취급자 및 이용자 등이 입력한 비밀번호를 평문형태가 아닌 해쉬함수를 통해 얻은 결과 값으로 시스템에 저장(일방향 암호화)하여야 한다고 해설하고, 비밀번호를 암호화 할 때에는 국내·외 암호 연구 관련기관에서 사용 권고하는 안전한 암호 알고리즘으로 암호화하여 저장하도록 한다고 해설하며 MD5, SHA-1 등 보안강도가 낮은 것으로 판명된 암호 알고리즘을 사용하여서는 안된다(2016.9월 기준)고 해설하고 있다.

다. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다."라고 규정하고 있다.

2. 위법성 판단

가. 개인정보의 이전{정보통신망법 제26조(영업의 양수 등에 따른 개인정보의 이전)} **시 이용자에게 통지를 소홀히 한 행위**

18 피심인이 2019. 2. 25. 로부터 사이트( ) 및 사이트 내 이용자 정보 일체를 양수 받으면서 그 사실과 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편, 서면, 모사전송, 전화 등의 방법으로 이용자에게 알리지 않은 행위는 정보통신망법 제26조제2항을 위반한 것이다.

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

19 **(안전한 인증수단)** 피심인이 외부에서 피심인의 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하고 추가적으로 안전한 인증수단(ex. 보안토큰, 휴대폰인증, 일회용 비밀번호, 바이오정보, 단말기 IP인증 등)을 적용하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제4항을 위반한 것이다.

20 **(침입탐지 시스템 설치·운영)** 피심인이 개인정보처리시스템에 접속한 IP 등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는 기능을 포함한 침입탐지시스템을 설치·운영하지 아니한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

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

21 피심인이 이용자의 비밀번호를 저장하면서 이를 복호화 되지 아니하도록 일방향 암호화(해쉬함수, 112비트 이상 보안강도)하여 저장하지 않은 행위는, 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제1호, 고시 제6조제1항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	이전 통지	§26②	-	개인정보를 이전받으면서 이용자에게 이전을 원하지 않을 경우 동의 철회방법과 절차를 제공하지 아니한 행위
	접근 통제	§28①2호	§15②2호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④)
				개인정보처리시스템에 침입탐지시스템 설치·운영하지 아니한 행위(고시§4⑤)
	암호화	§28①4호	§15④1호	이용자의 비밀번호를 안전하지 않은 암호알고리즘으로 암호화하여 저장한 행위(고시§6①)

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보를 이전받으면 지체 없이 그 사실 및 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편, 서면, 모사전송, 전화 등의 방법으로 이용자에게 알려야 한다.

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)개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 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) 비밀번호는 복호화 되지 아니하도록 안전한 암호알고리즘을 이용하여 일방향 암호화하여 저장할 것

2. 시정명령 이행결과의 보고

22 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. 과태료 부과

23 피심인의 정보통신망법 제26조(영업의 양수 등에 따른 개인정보의 이전)제2항, 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 법제76조제2항제2호, 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

24 정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하므로 정보통신망법 제26조제2항 위반에 대해서 1회 위반 과태료인 600만원을 적용하고, 같은 법 제28조제1항 위반에 대해서 1회 위반 과태료인 1,000만원을 적용한다.

〈 위반 횟수별 과태료 금액 〉

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
카. 법 제26조제1항 및 제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보 이전 사실을 알리지 않은 경우	법 제76조 제2항제2호	600	1,200	2,000
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 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.

25 이에 따라 피심인의 정보통신망법 제28조1항 위반행위는 위반행위별 각 목의 세부기준에서 정한 행위가 2개인 경우에 해당하므로 기준금액의 30%인 300만원을 가중하고, 같은 법 제26조제2항 위반행위는 특별히 가중할 사유가 없으므로 기준금액을 유지한다.

< 과태료 부과지침 [별표2] '과태료의 가중기준' >

기준	가중사유	가중비율
위반의 정도	나. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내
	제3호 정보통신망법 시행령 제74조 별표 9 제2호 너목 가. 정보통신망법 제28조제1항제1호에 따른 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행을 하지 않은 경우 나. 정보통신망법 제28조제1항제2호에 따른 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 하지 않은 경우 다. 정보통신망법 제28조제1항제3호에 따른 접속기록의 위조·변조 방지를 위한 조치를 하지 않은 경우 라. 정보통신망법 제28조제1항제4호에 따른 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하지 않은 경우 마. 정보통신망법 제28조제1항제5호에 따른 백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지조치를 하지 않은 경우 바. 정보통신망법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치를 하지 않은 경우	

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.

26 이에 따라 피심인의 정보통신망법 제28조제1항 위반행위는 시정조치(안) 사

전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 기준금액의 50%인 500만원을 감경하고 같은 법 제26조제2항 위반행위는 특별히 감경할 사유가 없으므로 기준금액을 유지한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§26②	600만원	없음	없음	**600만원**
§28①2·4호	1,000만원	300만원	500만원	**800만원**
계				**1,400만원**

다. 최종 과태료

27 이에 따라 피심인의 정보통신망법 제26조제2항, 제28조제1항 위반행위에 대해 14,000,000원의 과태료를 부과한다.

Ⅵ. 결론

28 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호, 제76조제2항제2호(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.

2020년 5월 19일

위 원 장 한 상 혁 (인)

부위원장 표 철 수 (인)

위 원 허 욱 (인)

위 원 김 창 룡 (인)

위 원 안 형 환 (인)