방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020 - 38 - 177호

안 건 명 개인정보 유출신고 사업자의 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020. 6. 24.

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

나. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리 적용할 것

다. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권

한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것

라. 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취할 것

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 과태료를 부과한다.

가. 금　　액 : 5,000,000원

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)는 영리를 목적으로 유·아동 물품 판매 쇼핑몰 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 : 백만원)

구 분	2016년	2017년	2018년	3년 평균
전체 매출				
관련 매출				
관련없는 매출				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

Ⅱ. 사실조사 결과

1. 조사 대상

2. 방송통신위원회는 온라인 개인정보보호 포털(i-privacy.kr)에 개인정보 유출을 신고한 피심인에 대하여 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 조사 하였고, 피심인에 대한 현장조사(2019. 5. 9.~5. 10., 7. 25.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

3. 피심인은 유·아동 물품 판매 온라인 쇼핑몰 를 .
1. 15.부터 운영하면서, 2019. 5. 10. 기준 이용자 건의 개인정보를 수집하여 보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구분	항목	수집일	건수
회원정보 (유효회원)	**통합회원(필수)** : 아이디, 비밀번호, 이름, 생년월일, 성별, 휴대폰 번호, 이메일 주소, 본인인증정보 **간편회원(필수)** : SNS 종류, SNS ID, 휴대폰 번호 **(선택)** : 주소, 결혼여부, 임신여부, SNS URL, 자녀정보(자녀유무, 자녀수, 자녀이름, 자녀, 생년월일, 자녀 성별)		건
(휴면회원)	상동		건
총계			**건**

나. 개인정보 유출 경위

1) 개인정보 유출 경과 및 대응

- 2019.4.9. 고객센터로 타인의 개인정보가 조회된다는 민원 접수를 통해 개인정보 유출 사실 인지(민원 접수 4건)
- 2019.4.10. 민원 접수된 4건 중 1건에 대해 개인정보 유출 사실 통지
- 2019.4.10. 개인정보보호 포털(i-privacy.kr)에 개인정보 유출 신고(1차)

※ 개인정보 유출여부가 확인되지 않아 유출발생 원인 파악 후 이용자 통지 및 신고

- 2019.4.17. 구글 분석기의 패턴 분석을 통한 개인정보 유출 사실 확인
- 2019.4.18.~30. 개인정보보호 포털(i-privacy.kr)에 개인정보 유출 신고(2차)

※ 2019.4.18.(6건), 4.24.(11건), 4.30.(3건)에 대하여 전화 또는 SMS 안내 완료

※ 2019.4.18.~30.까지 고객센터 추가 인입 및 분석 후 3회에 걸쳐서 추가 유출 신고

- 2019.4.18. 02:00 시스템 문제점으로 판단되는 JBOSS 패치 및 보안소스 강화 진행
- 2019.4.24. 시스템 패치 후에도 지속적인 민원 발생으로 서비스 일시 중지
- 2019.4.29 시스템 2차 패치 및 추가 보안 강화를 후 시스템 정상 운영

2) 개인정보 유출 규모

4. 피심인의 회원정보(이름, 배송지 주소, 전화번호, 이메일 등) 21건이 유출되었다.

< 피심인의 개인정보 유출현황 >

구 분	유 출 항 목	건 수
맘큐 회원정보	이름, 배송지 주소, 전화번호, 이메일 등	21건

3) 유출 경로

5. 피심인이 운영하고 있는 전체 서비스를 이용하기 위해 제공되는 SSO* 회원 로그인 서비스와 회원 로그인 서비스를 2015. 12. 2.부터 연동하고 있었으며, 2019. 4. 9.부터 WAS(Web Application System)서버에서 개인을 식별하는 인증정보(쿠키, 세션 등)를 생성·전달하는 과정에서 시스템 오류가 발생하여 타인의 개인정보가 조회·유출됨

* SSO(Single-Sign-On) : 피심인이 운영 중인 서비스를 하나의 계정으로 1회 로그인을 통해 모두 이용할 수 있도록 제공하는 통합 로그인 기능

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

1) 피심인은 2019. 5. 10. 기준, 외부 인터넷망에서 홈페이지 관리자페이지 에 접속하는 개인정보취급자가 인증서·SMS인증·OTP 등의 추가적인 안전한 인증수단이 없이 ID, 비밀번호만으로 접속 가능하도록 운영한 사

실이 있다.

2) 피심인은 2019. 5. 10. 기준 망분리 대상 개인정보취급자가 개인정보처리시스템에 접속하기 위해 VD(가상머신) 환경을 구축·운영하고 있으며, 개인정보취급자는 인터넷망에 연결된 PC에서 SSL-VPN(ID, PW, OTP 인증)을 이용하여 개인정보처리시스템에 접속하고 있었으나, 개인정보취급자가 VD에서 다운로드한 개인정보 파일을 PC로 다운로드 시 망간자료전송 통제 없이 전송이 가능하였으며, 외부 인터넷 접속이 제한되지 않아 상용 메일을 이용하여 개인정보 파일을 외부로 전송할 수 있도록 운영한 사실이 있다.

3) 피심인이 서비스 운영을 위해 사용 중인 JBOSS WAS 서버가 세션 정보를 생성하는 과정에서 오작동하여 타 세션 정보가 잘못 생성되었고 타인의 개인정보가 조회된 사실이 있다.

4) 피심인은 2019. 5. 10. 기준 개인정보취급자가 개인정보처리시스템 접속하여 2시간 이상 업무처리를 하지 않은 경우에 한하여 자동으로 접속이 차단(로그아웃)되도록 설정한 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

6. 방송통신위원회는 2019. 11. 13. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 12. 4. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 처

리할 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.

7. 정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(개인정보처리스템)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)', '전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자의 경우 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등의 조치를 하여야 한다."라고 규정하고 있다.

8. 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 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."라고 규정하고 있고, 제4조제6항은 "전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다."고 규정하고 있으며, 제4조제9항은 "정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라

고 규정하고 있다. 제4조제10항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다."라고 규정하고 있다.

9. '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 있고, 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 있고, 제4조제6항에 대해 개인정보처리시스템에 접근하여 다운로드, 파기 또는 접근권한 설정이 가능한 개인정보취급자는 외부 인터넷망이 차단된 업무망에서 업무를 수행하여야 하며, 업무망과 외부 인터넷망은 서로의 영역에 접근할 수 없도록 물리적이나 논리적으로 망분리하여 차단하여야 한다고 해설하고 있다. 또한 정보통신서비스 제공자등을 위한 망분리 해설에서 논리적 망분리는 일반적으로 물리적 망분리에 비해 상대적으로 보안성이 떨어질 수 있으므로 업무망과 인터넷망 간의 자료 전송이 필요할 때에는 망연계 시스템 등 방법이 활용될 수 있다고 해설하고 있다.

10. 제4조제9항에 대해 인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해

정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 하며, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 보호조치를 하여야 한다고 해설하며, 인터넷 홈페이지 설계 시 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 ①입력 데이터의 유효성을 검증, ②인증, 접근통제 등의 보호조치 적용, ③에러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성, ④세션을 안전하게 관리하도록 구성 등 필요한 보안대책을 마련하여야 한다고 해설하고 있다.

11. 제4조10항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않을 때에는 자동으로 시스템 접속이 차단되도록 최대 접속시간 제한 등의 조치를 취하여야 한다고 해설하며, 최대 접속시간 제한 조치는 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속을 차단하는 것을 의미하며, 최대 접속시간이 경과하면 개인정보처리시스템과 연결이 완전히 차단되어 정보의 송·수신이 불가능한 상태가 되어야 한다고 해설하고 있다. 또한 최대 접속시간은 최소한(통상 10~30분 이내)으로 정하여야 한다. 다만, 장시간 접속이 필요할 때에는 접속시간 등 그 기록을 보관·관리하여야 한다고 해설하고 있다.

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

1) (안전한 인증수단) 피심인이 개인정보취급자가 외부 인터넷망에서 피심인의 개인정보처리시스템 에 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 제15조제2항제2호, 고시 제4조제4항을 위반한 것이다.

2) (망분리) 피심인은 망분리 대상 개인정보취급자가 개인정보처리시스템에 접속하기 위해 가상머신(VD) 환경을 구축·운영하고 있으나 개인정보취급자가 가상머신(VD)에서 다운로드한 개인정보 파일을 PC로 다운로드 시 망간자료전송 통제 없이 전송이 가능하도록 운영한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제3호, 고시 제4조제6항을 위반한 것이다.

3) (개인정보 유·노출 방지) 피심인이 홈페이지에서 개인을 식별하는 인증정보(쿠키, 세션 등)가 에러, 오류 처리되지 않거나 불충분하게 처리되지 않도록 구성하지 않아 피심인의 홈페이지에서 취급중인 개인정보가 열람권한 없는 자에게 공개(노출)되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

4) (최대 접속시간) 피심인이 개인정보취급자의 접속시간이 필요한 시간 동안만 최대 접속시간 제한(통상10~30분 이내) 등의 조치를 취하지 않고 2시간 이상 업무처리를 하지 않은 경우에 한하여 자동으로 접속이 차단(로그아웃)되도록 설정·운영한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제10항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②2호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증 수단을 적용하지 아니한 행위(고시§4④)
	접근 통제	§28①2호	§15②3호	개인정보 다운로드 및 파기 가능한 개인정보취급자의 컴퓨터를 망분리 적용하지 아니한 행위(고시§4⑥)
	접근 통제	§28①2호	§15②5호	열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)
	접근 통제	§28①2호	§15②5호	개인정보취급자의 접속시간이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하지 않은 행위(고시§4⑩)

Ⅳ. 시정조치 명령

1. 시정명령

12. 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)개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리 적용할 것 3)취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것 4)개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취할 것

2. 시정명령 이행결과의 보고

13. 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

14. 피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표 9] 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

15. 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 1회 위반 과태료인 1,000만원을 적용한다.

〈 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

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 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

16. 그러나 피심인은 특별히 해당사항이 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 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

17. 이에 따라 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 기준금액의 50%인 1,000만원을 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①2호	1,000만원	없음	500만원	**500만원**
계				**500만원**

다. 최종 과태료

18. 이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 5,000,000

원의 과태료를 부과한다.

Ⅵ. 결론

19. 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

20. 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.

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

22. 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 6월 24일

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)